

Konfigurieren von Wireshark und FreeRADIUS zur Entschlüsselung des 802.11 WPA2-Enterprise/EAP/dot1x Wireless-Sniffers über die Funkverbindung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Vorgehensweise](#)

[Schritt 1: Entschlüsseln von PMK\(s\) aus dem Access-Accept-Paket.](#)

[Schritt 2: PMK\(s\) extrahieren.](#)

[Schritt 3: Entschlüsseln Sie den OTA-Sniffer.](#)

[Beispiel für ein entschlüsseltes 802.11-Paket](#)

[Beispiel für ein verschlüsseltes 802.11-Paket](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird die Entschlüsselung des verschlüsselten WLAN Protected Access 2 - Enterprise (WPA2-Enterprise)- oder 802.1x (dot1x)-verschlüsselten OTA-Sniffers (Wireless over the Air) mit allen Extensible Authentication Protocol (EAP)-Methoden beschrieben.

Es ist relativ einfach, PSK-basierte/WPA2-Personal 802.11 OTA-Erfassung zu entschlüsseln, solange die vollständigen EAP over LAN (EAPoL)-Handshakes erfasst werden. Pre-Shared Key (PSK) wird jedoch nicht immer aus Sicherheitsgründen empfohlen. Ein hartkodierte Passwort zu knacken ist nur eine Frage der Zeit.

Daher entscheiden sich viele Unternehmen für dot1x mit Remote Authentication Dial-In User Service (RADIUS) als bessere Sicherheitslösung für ihr Wireless-Netzwerk.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FreeRADIUS mit installiertem **Radsniff**
- Wireshark/Omnipeek oder eine Software, die 802.11-Wireless-Datenverkehr entschlüsseln kann

- Berechtigung zum Abrufen des gemeinsam genutzten geheimen Codes zwischen Netzwerkzugriffsserver (NAS) und Authentifizierer
- Erfassung der Radius-Paketerfassung zwischen NAS und Authentifizierer von der ersten Zugriffsanforderung (von NAS zu Authentifizierer) bis zur letzten Zugriffsgenehmigung (vom Authentifizierer zu NAS) während der gesamten EAP-Sitzung
- Möglichkeit zur OTA-Erfassung (Over-the-Air) mit vierseitigen EAPoL-Handshakes

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Radius-Server (FreeRADIUS oder ISE)
- Over-the-Air-Erfassungsgerät
- Apple MacOS/OS X- oder Linux-Gerät

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In diesem Beispiel werden zwei paarweise Master Keys (PMKs) von Radius-Paketen abgeleitet, die von ISE 2.3 erfasst wurden, da die Sitzungs-Timeout-Einstellung für diese SSID 1800 Sekunden beträgt und die hier angegebene Erfassung 34 Minuten (2040 Sekunden) lang ist.

Wie im Bild gezeigt, wird EAP-PEAP als Beispiel verwendet, kann jedoch auf jede dot1x-basierte Wireless-Authentifizierung angewendet werden.

No.	Time	Source	Destination	Protocol	Length	Info
4325	2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	EAP	109	Request, TLS EAP (EAP-TLS)
4327	2018-11-16 00:04:02.812927	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Legacy Nak (Response Only)
4329	2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	EAP	109	Request, Protected EAP (EAP-PEAP)
4332	2018-11-16 00:04:02.818331	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSPv1.2	244	Client Hello
4349	2018-11-16 00:04:02.828460	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	1079	Server Hello, Certificate, Server Key Exchange, Server Hell
4352	2018-11-16 00:04:02.829281	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Protected EAP (EAP-PEAP)
4354	2018-11-16 00:04:02.833165	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	1075	Server Hello, Certificate, Server Key Exchange, Server Hell
4356	2018-11-16 00:04:02.834110	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Protected EAP (EAP-PEAP)
4361	2018-11-16 00:04:02.839052	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	738	Server Hello, Certificate, Server Key Exchange, Server Hell
4363	2018-11-16 00:04:02.845892	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSPv1.2	199	Client Key Exchange, Change Cipher Spec, Encrypted Handshak
4365	2018-11-16 00:04:02.851843	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	124	Change Cipher Spec, Encrypted Handshake Message
4367	2018-11-16 00:04:02.853063	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Protected EAP (EAP-PEAP)

No.	Time	Source	Destination	Protocol	Length	Info
9095_	2018-11-16 00:34:07.507960	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	754	Encrypted Handshake Message, Encrypted Handshake Message, E
9095_	2018-11-16 00:34:07.519109	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSPv1.2	215	Encrypted Handshake Message, Change Cipher Spec, Encrypted
9095_	2018-11-16 00:34:07.524344	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	140	Change Cipher Spec, Encrypted Handshake Message
9095_	2018-11-16 00:34:07.525423	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	89	Response, Protected EAP (EAP-PEAP)
9095_	2018-11-16 00:34:07.528660	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	125	Application Data
9095_	2018-11-16 00:34:07.529567	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSPv1.2	129	Application Data
9095_	2018-11-16 00:34:07.532409	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	151	Application Data
9095_	2018-11-16 00:34:07.536570	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSPv1.2	183	Application Data
9095_	2018-11-16 00:34:07.569469	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	169	Application Data
9095_	2018-11-16 00:34:07.570964	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	TLSPv1.2	124	Application Data
9095_	2018-11-16 00:34:07.574596	Cisco_b4:3d:e4	HmdGlobo_6a:69:11	TLSPv1.2	125	Application Data
9095_	2018-11-16 00:34:07.575693	HmdGlobo_6a:69:11	Cisco_b4:3d:e4	EAP	89	Response, Protected EAP (EAP-PEAP)

Vorgehensweise

Schritt 1: Entschlüsseln von PMK(s) aus dem Access-Accept-Paket.

Tip: Im Allgemeinen kann die Laufzeit des Befehls **radsniff** für eine RADIUS pcap-Datei als Sekunden gezählt werden. Wenn der **Radsniff** jedoch in diesem im Protokoll angezeigten Zustand feststeckt, kaskadieren Sie diese Paketerfassung (A) mit einer weiteren längeren Paketerfassung (B) zwischen demselben NAS und Authentifizierer. Führen Sie dann den Befehl **radsniff** für das kaskadierte Paket (A+B) aus. Die einzige Anforderung für die Paketerfassung (B) besteht darin, dass Sie den Befehl **radsniff** darauf ausführen und das ausführliche Ergebnis anzeigen können.


```
FRLU-M-51X5:pcaps frlu$ radsniff -I /Users/frlu/Downloads/radius_novlan.pcap -s Cisco123 -x
```

```
Logging all events
```

```
Sniffing on (/Users/frlu/Downloads/radius_novlan.pcap)
```

In diesem Beispiel wird die Protokollierung der Steuerungsebene (A), die über die [WLC-Paketprotokollierungsfunktion](#) erfasst wird, mit einer längeren Erfassung von TCPdump (B) der ISE kaskadiert. Die Protokollierung von WLC-Paketen dient als Beispiel, da sie in der Regel sehr klein ist.

WLC-Paketprotokollierung (A)

 radius_novlan.pcap	Pcap N...apture	22 KB	Today at 11:56 am
--	-----------------	-------	-------------------

ISE Tcpdump (B)

 radius_eap_decode_Cisco123.pcap	Yesterday at 12:04 pm	850 KB	Pcap N...apture
---	-----------------------	--------	-----------------

Zusammengeführt (A+B)

 radius_novlan_merged.pcapng	Pcapn...Capture	927 KB	Today at 12:28 pm
---	-----------------	--------	-------------------

Führen Sie dann den **Radsniff** gegen das zusammengeführte pcap aus (A+B), und Sie können die ausführliche Ausgabe sehen.

```
FRLU-M-51X5:pcaps frlu$ radsniff -I /Users/frlu/Downloads/radius_novlan_merged.pcapng -s  
<shared-secret between NAS and Authenticator> -x
```

```
<snip>
```

```
2018-11-16 11:39:01.230000 (24) Access-Accept Id 172  
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000  
+0.000
```

```
<snip>
```

Schritt 2: PMK(s) extrahieren.

Löschen Sie in jedem **MS-MPPE-Recv-Key** aus der ausführlichen Ausgabe das 0x-Feld, und die PMKs, die für die Wireless-Datenverkehrsdekodierung erforderlich sind, werden angezeigt.

```
MS-MPPE-Recv-Key = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a  
066d8b3b
```

PMK :

d4b0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

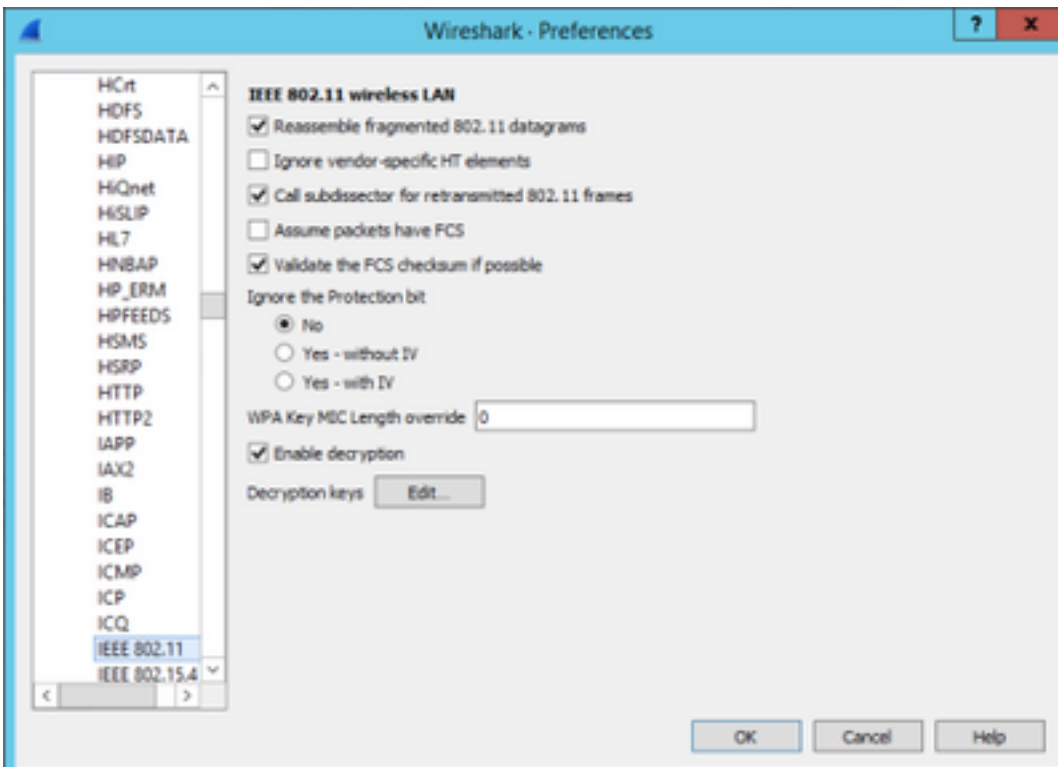
MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4fb1ccb0e

PMK :

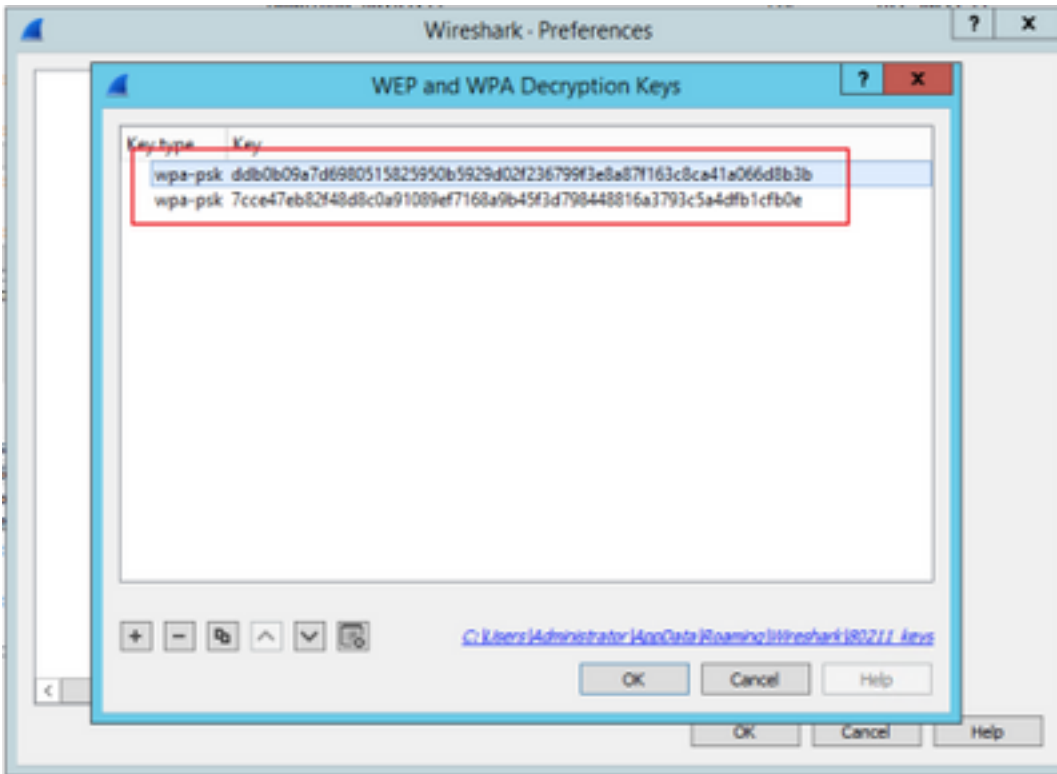
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

Schritt 3: Entschlüsseln Sie den OTA-Sniffer.

Navigieren Sie zu **Wireshark > Preferences > Protocols > IEEE 802.11**. Tippen Sie dann auf **Entschlüsselung aktivieren** und klicken Sie auf die Schaltfläche **Bearbeiten** neben **Entschlüsselungsschlüssel**, wie im Bild gezeigt.



Wählen Sie anschließend **wpa-psk** als Key-Typ aus, legen Sie die abgeleiteten PMKs in das **Key-**Feld ein, und klicken Sie dann auf **OK**. Nach Abschluss dieses Vorgangs sollte die OTA-Erfassung entschlüsselt werden, und Sie können Informationen auf höherer Ebene (3+) anzeigen.



Beispiel für ein entschlüsseltes 802.11-Paket

No.	Time	Source	Destination	Protocol	Length	Info
397877	2018-11-16 00:17:08.095884	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T...	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	45	Request-to-send, Flags=.....C
397879	2018-11-16 00:17:08.097877	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T...	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	45	Request-to-send, Flags=.....C
397881	2018-11-16 00:17:08.098393	40.127.66.24	172.16.255.13	TCP	1438	[TCP Retransmission] 80 → 45658 [ACK] Seq=3999900
397882	2018-11-16 00:17:08.098444	104.17.57.239	172.16.255.13	TCP	154	80 → 37553 [ACK] Seq=1 Ack=310 Win=65344 Len=0 TS
397883	2018-11-16 00:17:08.098495	HmdGloba_6a:69:11 (04:f1:28:6a:69:11)...	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
397884	2018-11-16 00:17:08.098999	104.17.57.239	172.16.255.13	TCP	162	80 → 37555 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
397886	2018-11-16 00:17:08.099099	172.16.255.13	40.127.66.24	TCP	154	45658 → 80 [ACK] Seq=128 Ack=4001196 Win=788480 L
397887	2018-11-16 00:17:08.099181	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T...	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
397888	2018-11-16 00:17:08.099606	172.16.255.13	104.17.57.239	TCP	154	37555 → 80 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSva
397889	2018-11-16 00:17:08.099655	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T...	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57	802.11 Block Ack, Flags=.....C
397890	2018-11-16 00:17:08.101762	172.16.255.13	104.17.57.239	HTTP	479	GET /s100264/images/logo.png?t=636366 HTTP/1.1
397891	2018-11-16 00:17:08.101812	Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (T...	HmdGloba_6a:69:11 (04:f1:28:6a:69:11) (RA)	802.11	57	802.11 Block Ack, Flags=.....C

Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
 Radiotap Header v0, Length 48
 802.11 radio information
 IEEE 802.11 QoS Data, Flags: .p.....TC
 Logical-Link Control
 Internet Protocol Version 4, Src: 172.16.255.13, Dst: 40.127.66.24
 Transmission Control Protocol, Src Port: 45658, Dst Port: 80, Seq: 128, Ack: 4001196, Len: 0

```

0000 00 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 00 00  ..0.k... m 01...
0010 14 00 9e 09 00 04 d9 a4 00 00 00 00 04 01 00  ....a.....
0020 9e 09 0b 22 1f 00 06 00 65 00 00 04 00 00 00  .........
0030 88 41 30 00 80 a3 8e b4 3d e4 04 f1 28 6a 69 11  A0 ..... (ji
0040 00 0c 29 28 89 dd 50 06 00 00 c8 84 00 20 01 00  ..) (-P.....
0050 00 00 af f4 c2 2f 90 d1 14 52 a5 8b 2e 57 27 3a  ....//..R...W':
0060 d8 54 a5 55 0a 12 92 da fc a9 1f c2 c8 34 39 ca  T.U.....49-
0070 5c 08 7a 36 57 cd e2 43 89 86 f5 92 24 17 d0 db  \z6m-C...$...
0080 42 a2 2e 62 35 c7 36 9b 54 d0 00 91 78 7d 44 87  B..b5-6-T...x)D
0090 23 6c 7b e6 fd db e7 06 39 11  #l{..... 9-
  
```

Wenn Sie das zweite Ergebnis vergleichen, bei dem der PMK nicht enthalten ist, mit dem ersten Ergebnis, bei dem der PMK enthalten ist, wird Paket 397886 als 802.11-QoS-Daten entschlüsselt.

Beispiel für ein verschlüsseltes 802.11-Paket

Vorsicht: Sie können bei der Entschlüsselung auf ein Problem mit Wireshark stoßen. Selbst wenn der richtige PMK bereitgestellt wird (oder wenn PSK verwendet wird, werden sowohl SSID als auch PSK bereitgestellt), entschlüsselt Wireshark die OTA-Erfassung nicht. Die Problemumgehung besteht darin, Wireshark ein- und mehrmals auszuschalten, bis höhere Layer-Informationen abgerufen werden können und 802.11-Pakete nicht mehr als QoS-Daten angezeigt werden, oder einen anderen PC/Mac zu verwenden, auf dem Wireshark installiert ist.

Tip: Ein C++-Code namens pmkXtract ist im ersten Beitrag in Related Information angehängt. Die zu kompilierenden Versuche wurden erfolgreich durchgeführt, und es wird eine ausführbare Datei abgerufen, aber das ausführbare Programm scheint die Entschlüsselung aus einigen unbekanntenen Gründen nicht ordnungsgemäß durchzuführen. Zusätzlich wird ein Python-Skript, das versucht, PMK zu extrahieren, im Kommentarbereich des ersten Beitrags veröffentlicht, der bei Interesse der Leser weiter erforscht werden kann.

Zugehörige Informationen

- [Optimierung der schwachen Verbindung von EAP - Entziehen von Wi-Fi-PMKs aus RADIUS mit pmkXtract](#)
- [Dekodieren des Radius MS-MPPE-Recv-Key](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)