

Wireless-shark en FreeRADIUS configureren voor het decrypteren van 802.11 WAP2-Enterprise/EAP/dot1x-luchtdraadloze snelkiezer

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Procedure](#)

[Stap 1. Versleutel PMK\(s\) van access-accepteer Packet.](#)

[Stap 2: PMK\(en\) uittrekken.](#)

[Stap 3. Ontdek de OTA-slang.](#)

[Voorbeeld van een gedecrypteerd 802.11 Packet](#)

[Voorbeeld van een versleuteld 802.11 Packet](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u Wi-Fi beschermde access 2 - Enterprise (WAP2-Enterprise) of 802.1x (dot1x) versleutelde Wireless-over-the-air (OTA) snuifje kunt decrypteren, met alle MAP-methoden (Extensible Verification Protocol).

Het is relatief gemakkelijk om op PSK gebaseerde/WAP2-persoonlijke 802.11 OTA-opname te decrypteren zolang de volledige viervoudige EAP over LAN (EAPoL)-handleidingen worden opgenomen. Vooraf gedeelde sleutel (PSK) wordt echter niet altijd vanuit veiligheidsoogpunt aanbevolen. Het is een kwestie van tijd om een hard gecodeerd wachtwoord in te trekken.

Vandaar dat veel ondernemingen kiezen voor dot1x met afstandsverificatie Dial-In User Service (RADIUS) als een betere beveiligingsoplossing voor hun draadloze netwerk.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FreeRADIUS met **radsniff** geïnstalleerd
- Wireshark/Omnipeek of alle software die 802.11 draadloos verkeer kan decrypteren
- Bevoegd om het gedeelde geheim tussen netwerk access server (NAS) en Authenticator te verkrijgen
- Mogelijkheid om Straal pakketvastlegging tussen NAS en authenticator op te nemen van het

eerste toegangsverzoek (van NAS tot Authenticator) tot het laatste toegangsaanvaarden (van Authenticator tot NAS) gedurende de MAP-sessie

- Mogelijkheid om OTA-opname (over-the-Air) uit te voeren die viervoudige EAPoL-handschoenen bevat

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Radius-server (FreeRADIUS of ISE)
- Luchtvanger
- Apple Max/OS/X of Linux-apparaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

In dit voorbeeld worden twee Pairwise Master Keys (PMKs) afgeleid van Radius-pakketten die zijn opgenomen van ISE 2.3, omdat de sessietijd op deze SSID 1800 seconden is en de hier gegeven opname 34 minuten (2040 seconden) lang is.

Zoals in de afbeelding wordt getoond, wordt EAP-PEAP als voorbeeld gebruikt, maar dit kan worden toegepast op elke op dot1x gebaseerde draadloze authenticatie.

Network traffic capture showing EAP-PEAP handshake steps. The table below summarizes the key packets highlighted in red in the image:

No.	Time	Source	Destination	Protocol	Length	Info
4325	2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP	109	Request, TLS EAP (EAP-TLS)
4327	2018-11-16 00:04:02.812927	HmdGloba_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	HmdGloba_6a:69:11	EAP	109	Request, Protected EAP (EAP-PEAP)
4332	2018-11-16 00:04:02.818331	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	244	Client Hello
4349	2018-11-16 00:04:02.828460	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	1079	Server Hello, Certificate, Server Key Exchange, Server Hell
4352	2018-11-16 00:04:02.829281	HmdGloba_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	HmdGloba_6a:69:11	TLSv1.2	1075	Server Hello, Certificate, Server Key Exchange, Server Hell
4356	2018-11-16 00:04:02.834110	HmdGloba_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	HmdGloba_6a:69:11	TLSv1.2	738	Server Hello, Certificate, Server Key Exchange, Server Hell
4363	2018-11-16 00:04:02.845892	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	199	Client Key Exchange, Change Cipher Spec, Encrypted Handshak
4365	2018-11-16 00:04:02.851843	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	124	Change Cipher Spec, Encrypted Handshake Message
4367	2018-11-16 00:04:02.853063	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73	Response, Protected EAP (EAP-PEAP)

Network traffic capture showing EAP-PEAP application data and response. The table below summarizes the key packets highlighted in red in the image:

No.	Time	Source	Destination	Protocol	Length	Info
9095_	2018-11-16 00:34:07.507960	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	754	Encrypted Handshake Message, Encrypted Handshake Message, E
9095_	2018-11-16 00:34:07.519109	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	215	Encrypted Handshake Message, Change Cipher Spec, Encrypted
9095_	2018-11-16 00:34:07.524344	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	140	Change Cipher Spec, Encrypted Handshake Message
9095_	2018-11-16 00:34:07.525423	HmdGloba_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	HmdGloba_6a:69:11	TLSv1.2	125	Application Data
9095_	2018-11-16 00:34:07.529567	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	129	Application Data
9095_	2018-11-16 00:34:07.532409	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	151	Application Data
9095_	2018-11-16 00:34:07.536570	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	183	Application Data
9095_	2018-11-16 00:34:07.569469	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	169	Application Data
9095_	2018-11-16 00:34:07.570964	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSv1.2	124	Application Data
9095_	2018-11-16 00:34:07.574596	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	125	Application Data
9095_	2018-11-16 00:34:07.575693	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89	Response, Protected EAP (EAP-PEAP)

Procedure

Stap 1. Versleutel PMK(s) van access-accepteer Packet.

Draai de **radsniff** tegen Straalopname tussen NAS en Authenticator om PMK te extraheren. De reden waarom twee pakketten voor toegangscontrole tijdens de opname worden geëxtraheerd is dat de timer voor de sessie op deze specifieke SSID is ingesteld op 30 minuten en de opname 34

een schaal van seconden worden geteld. Als de raster echter vast zit in deze toestand die in het logbestand wordt weergegeven, noteert u deze pakketvastlegging (A) met een andere langere pakketvastlegging (B) tussen dezelfde NAS en Authenticator. Start vervolgens de radiofrequentie tegen het gecascadeerde pakje (A+B). Het enige vereiste van pakketvastlegging (B) is dat u de radiofunctie ertegen kunt uitvoeren en breedtegraden resultaat kunt zien.


```
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 dit voorbeeld wordt de controle-plane logging (WLC) van de draadloze LAN-controller (A) die wordt opgenomen via de functie [WLC pakketvastlegging](#), gecascadeerd met een langere opname van ISE's TCP-dumpen (B). De WLC pakketvastlegging wordt als voorbeeld gebruikt omdat het in omvang meestal zeer klein is.

WLC-pakketvastlegging (A)

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

ISE-tafelpomp (B)

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

Samengesteld (A+B)

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

Draai vervolgens de straal tegen het samengevoegde pcap (A+B) en u kunt de breedtegraad zien.

```
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>
```

Stap 2: PMK(en) uittrekken.

Verwijdert het 0x-veld in elke **MS-MPPE-Recv-Key** van de breedteuitvoer en de PMK's die nodig zijn voor de draadloze verkeersdecode, wordt vervolgens gepresenteerd.

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

```
PMK:
```

```
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

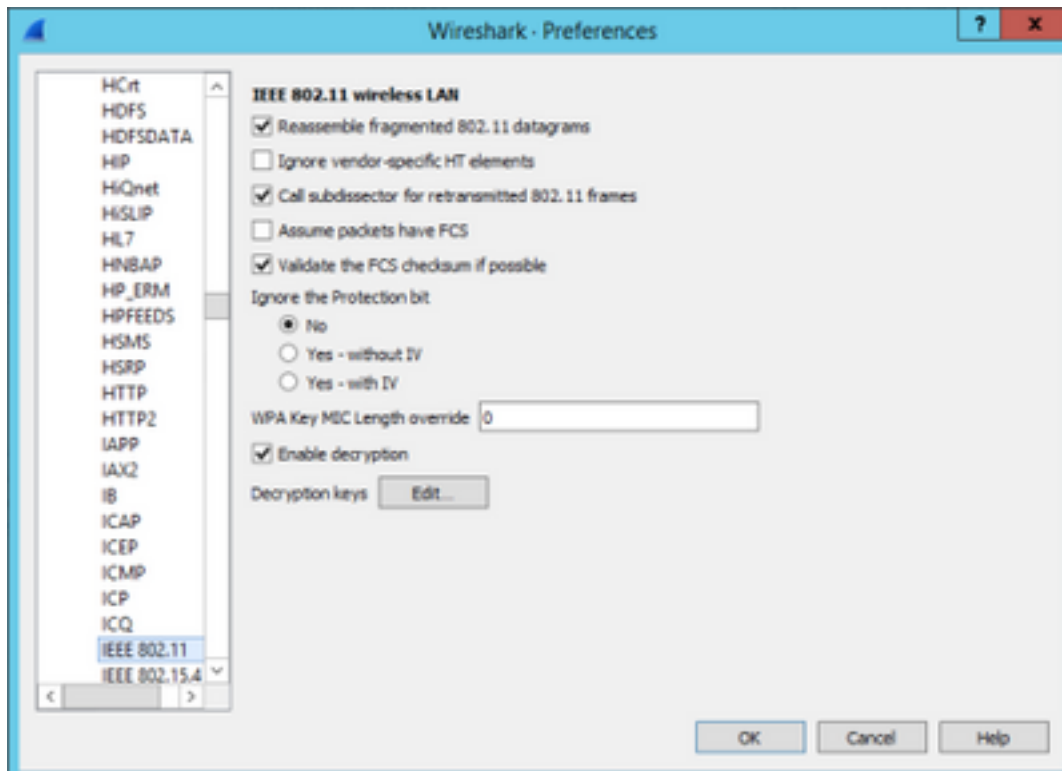
```
MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d7984816a3793c5a4dfb1b  
fb0e
```

PMK :

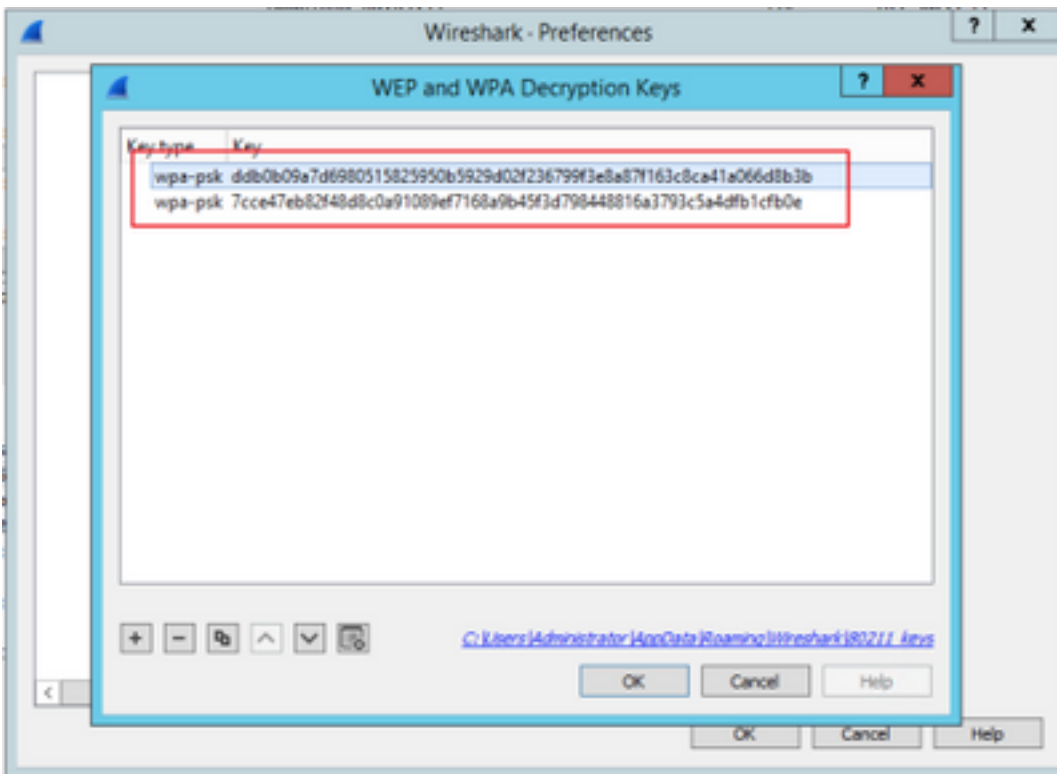
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

Stap 3. Ontdek de OTA-slang.

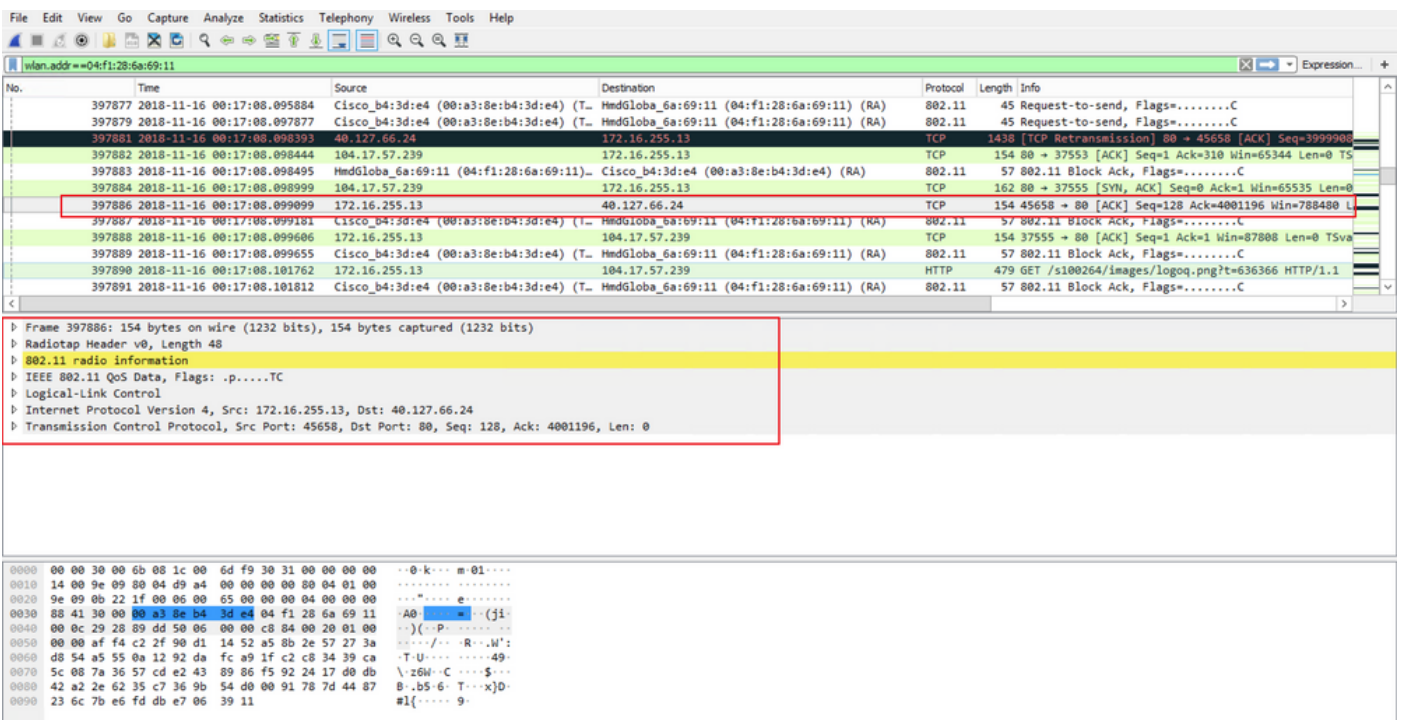
Navigeer naar **Wireless-shark > Voorkeuren > Protocols > IEEE 802.11**. Klik vervolgens op **Enable Decryption** en klik op de knop **Bewerken** naast **Decryptie-toetsen**, zoals in de afbeelding weergegeven.



Selecteer vervolgens **wpa-psk** als het Key type en zet de PMK's afgeleid in het **Key** veld, en klik vervolgens op **OK**. Nadat dit is voltooid, dient de OTA-opname te worden decrypteerd en kunt u informatie met een hogere laag (3+) zien.



Voorbeeld van een gedecrypteerd 802.11 Packet



Als u het tweede resultaat vergelijkt wanneer PMK niet is opgenomen, met het eerste resultaat, wanneer PMK is opgenomen, wordt pakket 397886 gedecrypteerd als 802.11 QoS gegevens.

Voorbeeld van een versleuteld 802.11 Packet

The screenshot displays the Wireshark interface with a packet capture of 802.11 QoS Data. The packet list pane shows several packets, with packet 397886 highlighted. The packet details pane shows the structure of the 802.11 radio information, including IEEE 802.11 QoS Data and Data (68 bytes). The packet bytes pane shows the raw hex and ASCII data.

Voorzichtig: U kunt bij decryptie problemen krijgen met Wireshark en in dat geval, zelfs als de juiste PMK is geleverd (of als PSK wordt gebruikt, zowel SSID als PSK worden geleverd), decrypteert Wireshark de OTA opname niet. Het programma is om Wireless-shark uit en op een paar keer uit te schakelen totdat meer laaginformatie kan worden verkregen en de pakketten 802.11 niet langer als QoS-gegevens worden weergegeven, of om een andere PC/Mac te gebruiken waar Wireless-shark is geïnstalleerd.

Tip: een C++ code genaamd pmkXtract is aangesloten in de eerste post op Gerelateerde informatie. Pogingen om samen te stellen werden succesvol en een uitvoerbaar bestand wordt verkregen, maar het uitvoerbare programma lijkt de decryptie niet goed uit te voeren om een paar onbekende redenen. Daarnaast is er een Python-script dat probeert PMK te extraheren in het commentaar op de eerste post, dat nader kan worden onderzocht indien de lezers geïnteresseerd zijn.

Gerelateerde informatie

- [De zwakke link van EAP bijsnijden - het zuigen van WiFi-PMK's met pmkXtract](#)
- [Hoe Decode Radius MS-MPPE-Recv-Key moet worden gedecodeerd](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)