

Configurez Wireshark et FreeRADIUS afin de déchiffrer l'analyseur sans fil 802.11 WPA2-Enterprise/EAP/dot1x en direct

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Procédure](#)

[Étape 1 : déchiffrement des PMK à partir du paquet Access-accept](#)

[Étape 2. Extraire les PMK.](#)

[Étape 3. Décryptage de l'analyseur OTA](#)

[Exemple de paquet 802.11 déchiffré](#)

[Exemple de paquet 802.11 chiffré](#)

[Informations connexes](#)

Introduction

Ce document décrit la procédure à suivre pour déchiffrer l'analyseur d'accès sans fil en direct (OTA) crypté Wi-Fi Protected Access 2 - Enterprise (WPA2-Enterprise) ou 802.1x (dot1x), avec toute méthode EAP (Extensible Authentication Protocol).

Il est relativement facile de décrypter la capture OTA 802.11 basée sur PSK/WPA2 personnel, à condition que les échanges EAPoL à quatre voies complets soient capturés. Cependant, la clé prépartagée (PSK) n'est pas toujours recommandée du point de vue de la sécurité. Il ne s'agit que d'une question de temps.

Par conséquent, de nombreuses entreprises choisissent dot1x avec Remote Authentication Dial-In User Service (RADIUS) comme meilleure solution de sécurité pour leur réseau sans fil.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FreeRADIUS avec **radsniff** installé
- Wireshark/Omnipeek ou tout logiciel capable de déchiffrer le trafic sans fil 802.11
- Privilège pour obtenir le secret partagé entre le serveur d'accès au réseau (NAS) et Authenticator
- Possibilité de capturer la capture de paquets radius entre le NAS et l'authentificateur à partir

de la première demande d'accès (du NAS à l'authentificateur) jusqu'à la dernière acceptation d'accès (de l'authentificateur au NAS) tout au long de la session EAP

- Possibilité d'effectuer une capture OTA (Over-the-Air) contenant des échanges EAPoL à quatre voies

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Serveur Radius (FreeRADIUS ou ISE)
- Périphérique de capture en vol
- Appareil Apple macOS/OS X ou Linux

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Dans cet exemple, deux clés maître par paire (PMK) sont dérivées de paquets Radius capturés à partir de ISE 2.3, car le délai d'attente de session sur ce SSID est de 1800 secondes et la capture donnée ici est de 34 minutes (2040 secondes).

Comme l'illustre l'image, EAP-PEAP est utilisé comme exemple, mais cela peut être appliqué à toute authentification sans fil basée sur dot1x.

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)

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)

Procédure

Étape 1 : déchiffrement des PMK à partir du paquet Access-accept

Exécutez le **radsniff** contre la capture radius entre NAS et Authenticator afin d'extraire PMK. La raison pour laquelle deux paquets d'acceptation d'accès sont extraits au cours de la capture est que le délai d'expiration de la session est défini sur 30 minutes sur ce SSID particulier et la

fichier pcap RADIUS peut être compté comme une échelle de secondes. Cependant, si le **radsniff** est coincé dans cet état indiqué dans le journal, mettez en cascade cette capture de paquets (A) avec une autre capture de paquets plus longue (B) entre le même NAS et l'authentificateur. Ensuite, exécutez la commande radsniff sur le paquet en cascade (A+B). La seule exigence de la capture de paquets (B) est que vous pouvez exécuter la commande radsniff contre elle et voir le résultat verbose.


```
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)
```

Dans cet exemple, la journalisation du plan de contrôle du contrôleur de réseau local sans fil (WLC) (A) capturée via la fonctionnalité de [journalisation des paquets du WLC](#), est en cascade avec une capture plus longue à partir du TCPdump (B) d'ISE. La journalisation des paquets WLC est utilisée comme exemple car elle est généralement de très petite taille.

Journalisation des paquets WLC (A)

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

Tcpdump ISE (B)

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

Fusion (A+B)

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

Ensuite, exécutez le **radsniff** contre le pcap fusionné (A+B) et vous pourrez voir la sortie du verbose.

```
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>
```

Étape 2. Extraire les PMK.

La suppression de 0x dans chaque **MS-MPPE-Recv-Key** à partir de la sortie détaillée et des PMK nécessaires au décodage du trafic sans fil est ensuite présentée.

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

```
PMK :  
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b  
MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d79848816a3793c5a4dfb1cb
```

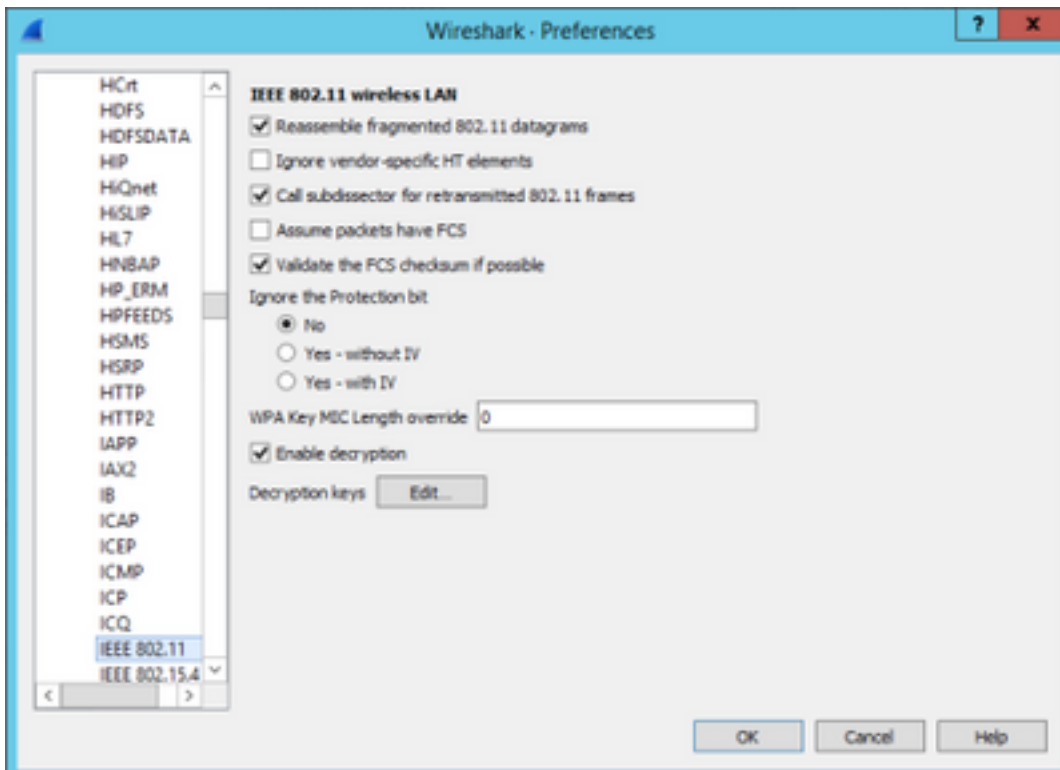
fb0e

PMK :

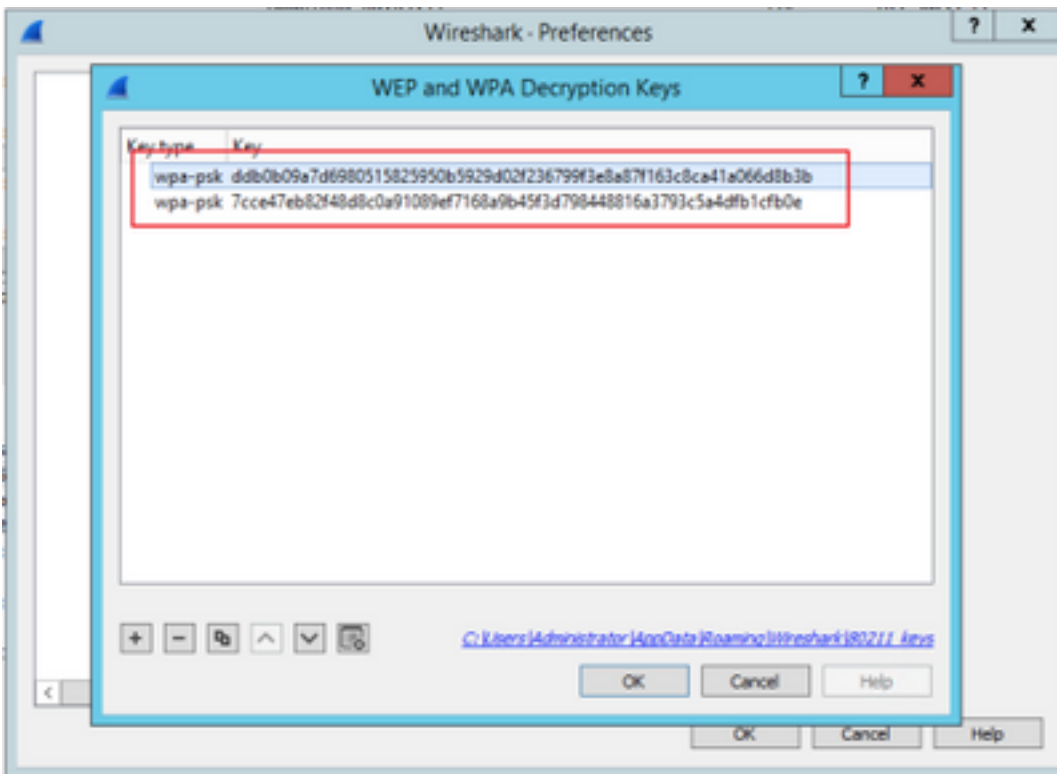
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

Étape 3. Décryptage de l'analyseur OTA

Accédez à **Wireshark > Préférences > Protocoles > IEEE 802.11**. Ensuite, cochez **Enable Decryption** et cliquez sur le bouton **Edit** en regard de **Decryption Keys**, comme indiqué dans l'image.



Ensuite, sélectionnez **wpa-psk** comme type de clé, puis placez les PMK dérivés dans le champ **Key**, puis cliquez sur **OK**. Une fois cette opération terminée, la capture OTA doit être déchiffrée et vous pouvez voir des informations de couche supérieure (3+).



Exemple de paquet 802.11 déchiffré

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=3999908
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

```

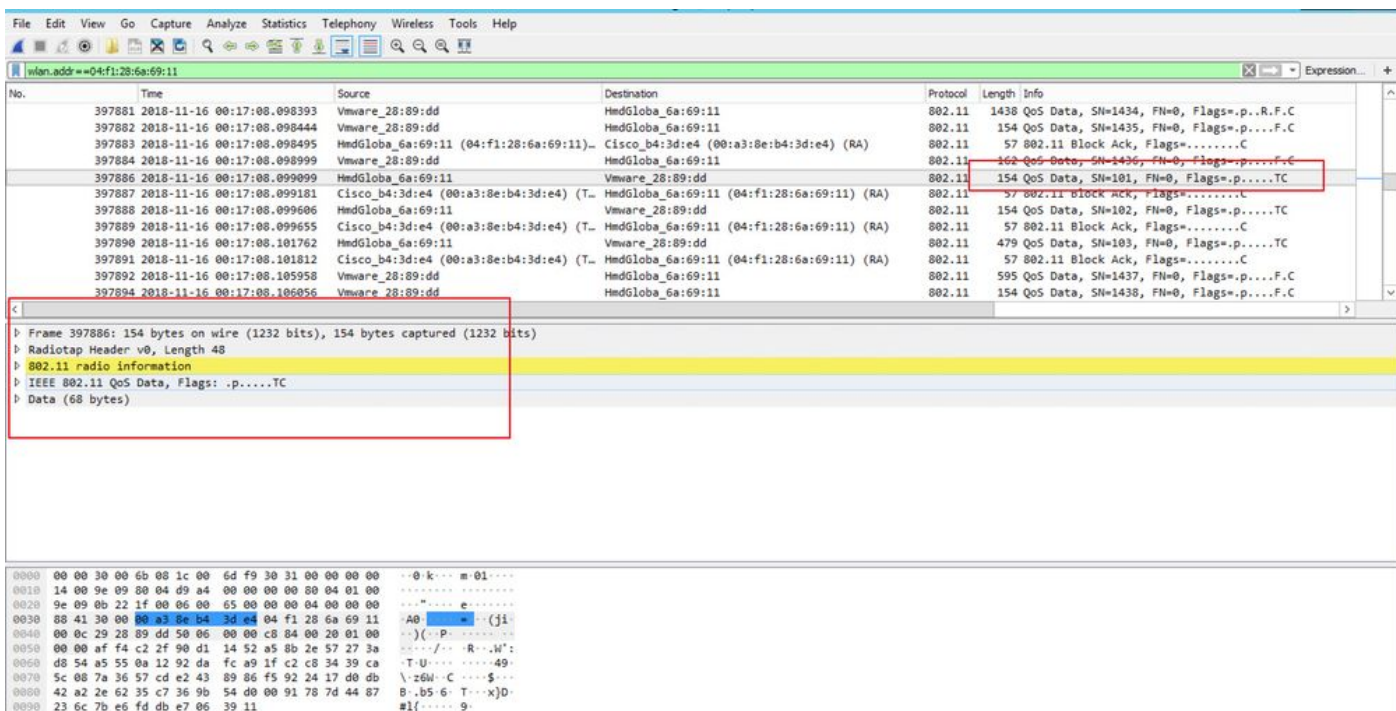
Frame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)
  Radiotap Header v0, Length 48
  802.11 radio information
  IEEE 802.11 QoS Data, Flags: .p.....TC
  Logical-Link Control
  Internet Protocol Version 4, Src: 172.16.255.13, Dst: 40.127.66.24
  Transmission Control Protocol,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

Si vous comparez le deuxième résultat où le PMK n'est pas inclus, avec le premier résultat, où le PMK est inclus, le paquet 397886 est déchiffré en données QoS 802.11.

Exemple de paquet 802.11 chiffré



Attention : Vous pouvez rencontrer un problème avec Wireshark lors du déchiffrement, et dans ce cas, même si le bon PMK est fourni (ou si PSK est utilisé, SSID et PSK sont fournis), Wireshark ne déchiffre pas la capture OTA. La solution de contournement consiste à désactiver Wireshark et à le désactiver plusieurs fois jusqu'à ce que des informations de couche supérieure puissent être obtenues et que les paquets 802.11 ne soient plus affichés comme des données QoS, ou à utiliser un autre PC/Mac sur lequel Wireshark est installé.

Conseil : Un code C++ appelé pmkXtract est joint dans le premier billet de la rubrique Informations connexes. Les tentatives de compilation ont été réussies et un fichier exécutable est obtenu, mais le programme exécutable ne semble pas effectuer le déchiffrement correctement pour certaines raisons inconnues. En outre, un script Python qui tente d'extraire PMK est publié dans la zone des commentaires sur le premier billet, qui peut être exploré plus avant si les lecteurs sont intéressés.

Informations connexes

- [Effacer le lien faible d'EAP : retirer les PMK WiFi de RADIUS avec pmkXtract](#)
- [Comment décoder Radius MS-MPPE-Recv-Key](#)
- [Support et documentation techniques - Cisco Systems](#)