設定Wireshark和FreeRADIUS以解密802.11 WPA2-Enterprise/EAP/dot1x over-the-air無線監聽器

目錄

簡介

本文說明如何使用任何可擴充驗證通訊協定(EAP)方法解密Wi-Fi保護存取2 — 企業（WPA2 — 企業）或802.1x(dot1x)加密的無線空中傳輸(OTA)監聽器。

只要擷取完整的4路EAP over LAN(EAPoL)交涉，解密基於PSK/WPA2個人802.11 OTA擷取相對容易。但是，從安全形度來看，並不總是建議使用預共用金鑰(PSK)。破解硬編碼密碼只是時間問題。

因此，許多企業選擇帶Remote Authentication Dial-In User Service(RADIUS)的dot1x作為其無線網路的更好安全解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- 安裝了**radsniff的**FreeRADIUS
- Wireshark/Omnipeek或能夠解密802.11無線流量的任何軟體
- 獲取網路訪問伺服器(NAS)和身份驗證器之間的共享密碼的許可權
- 能夠捕獲整個EAP會話中NAS和身份驗證器之間的radius資料包捕獲(從第一個訪問請求（從NAS到身份驗證器）到最後一個訪問接受（從身份驗證器到NAS）
- 能夠執行包含四路EAPoL握手的Over-the-Air(OTA)捕獲

採用元件

本文中的資訊係根據以下軟體和硬體版本：

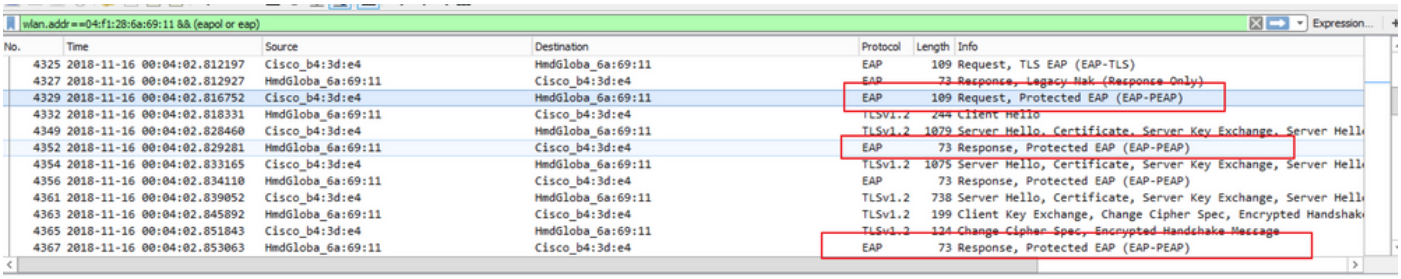
- Radius伺服器（FreeRADIUS或ISE）
- 空中捕捉裝置
- Apple macOS/OS X或Linux裝置

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

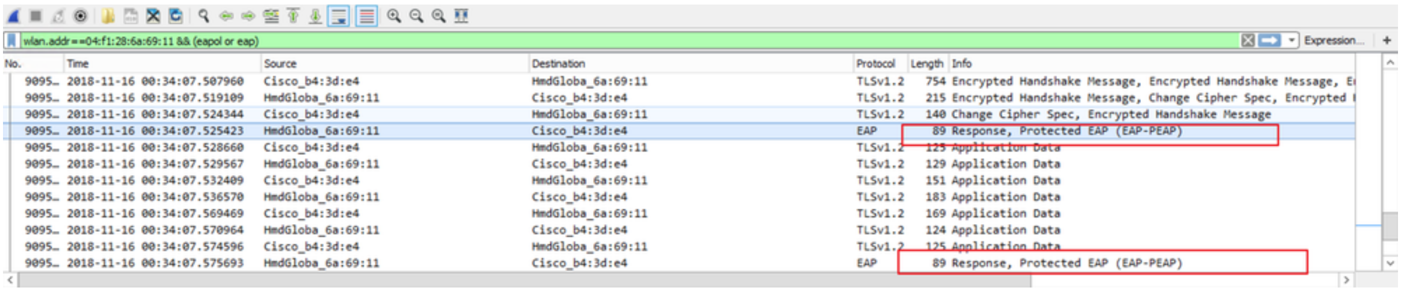
在本示例中，兩個成對主金鑰(PMK)源自從ISE 2.3捕獲的Radius資料包，因為此SSID上的會話超時為1800秒，此處給出的捕獲長度為34分鐘（2040秒）。

如圖所示，使用EAP-PEAP作為示例，但是這可以應用於任何基於dot1x的無線身份驗證。



wlan.addr==04:f1:28:6a:69:11 && (eapol or eap)

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)



wlan.addr==04:f1:28:6a:69:11 && (eapol or eap)

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)

程式

步驟1.從訪問接受資料包解密PMK。

在NAS和驗證器之間運行**radsniff**以捕獲radius，以提取PMK。在捕獲期間提取兩個訪問接受資料包的原因是，會話超時計時器在此特定SSID上設定為30分鐘，並且捕獲長達34分鐘。身份驗證執行兩次。

```
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
```

```
User-Name = "frlu_2"

State = 0x526561757468536573736f6e3a30613432346632613030303030356537356265653039373 2

Class =
0x434143533a30613432346632613030303030356537356265653039373 23a4953452d322d332f33323832373132333 8
2f33303432

EAP-Message = 0x03c50004

Message-Authenticator = 0x38c67b9ba349842c9624889a45cabdfb

MS-MPPE-Send-Key = 0xa464cc15c0df8f09edc249c28711eb13a6db2d1a176f1196edcc707579fd6793

MS-MPPE-Recv-Key =
0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b<<<<<<<<<<<<<<<<<<PMK

Authenticator-Field = 0x6cd33b4d4dde05c07d9923e17ad6c218

<snip>

2018-11-16 11:39:01.470000 (48) Access-Accept Id 183
/Users/frlu/Downloads/radius_novlan_merged.pcapng:10.66.79.42:32771 <- 10.66.79.36:1812 +0.000
+0.000

User-Name = "frlu_2"

State = 0x526561757468536573736f6e3a30613432346632613030303030356537356265653039373 2

Class =
0x434143533a30613432346632613030303030356537356265653039373 23a4953452d322d332f33323832373132333 8
2f33303434

EAP-Message = 0x03910004

Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9

MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb

MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e<<<<<<<<<<<<<<<<<PMK

Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

附註：請移除Radius封包擷取的任何虛擬LAN(VLAN)標籤，否則**radsniff** 無法識別輸入pcap檔案。若要移除任何VLAN標籤，例如，可以使用editcap。

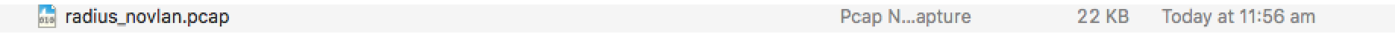
提示：通常，針對RADIUS pcap檔案的**radsniff**命令運行時可以計為秒數。但是，如果**radsniff**停滯在日誌中顯示的此狀態，請將此資料包捕獲(A)與同一NAS和身份驗證器之間的另一個較長資料包捕獲(B)進行級聯。然後，對級聯資料包(A+B)運行radsniff命令。 資料包捕獲(B)的唯一要求是，您可以對它運行radsniff命令並檢視詳細結果。

```
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)
```

在本範例中，透過WLC封包記錄功能擷取的無線Lan控制器(WLC)控制層面記錄(A)與ISE的TCPdump(B)中的較長擷取進行級聯。之所以使用WLC封包記錄作為範例，是因為它的大小通常非

常小。

WLC封包記錄(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

合併(A+B)

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

然後對合併的pcap(A+B)運行**radsniff**，您將能夠看到詳細輸出。

```
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>
```

步驟2.提取PMK。

然後，從詳細輸出中刪除每個**MS-MPPE-Recv-Key**中的0x欄位，並顯示無線業務解碼所需的PMK。

MS-MPPE-Recv-Key =
0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

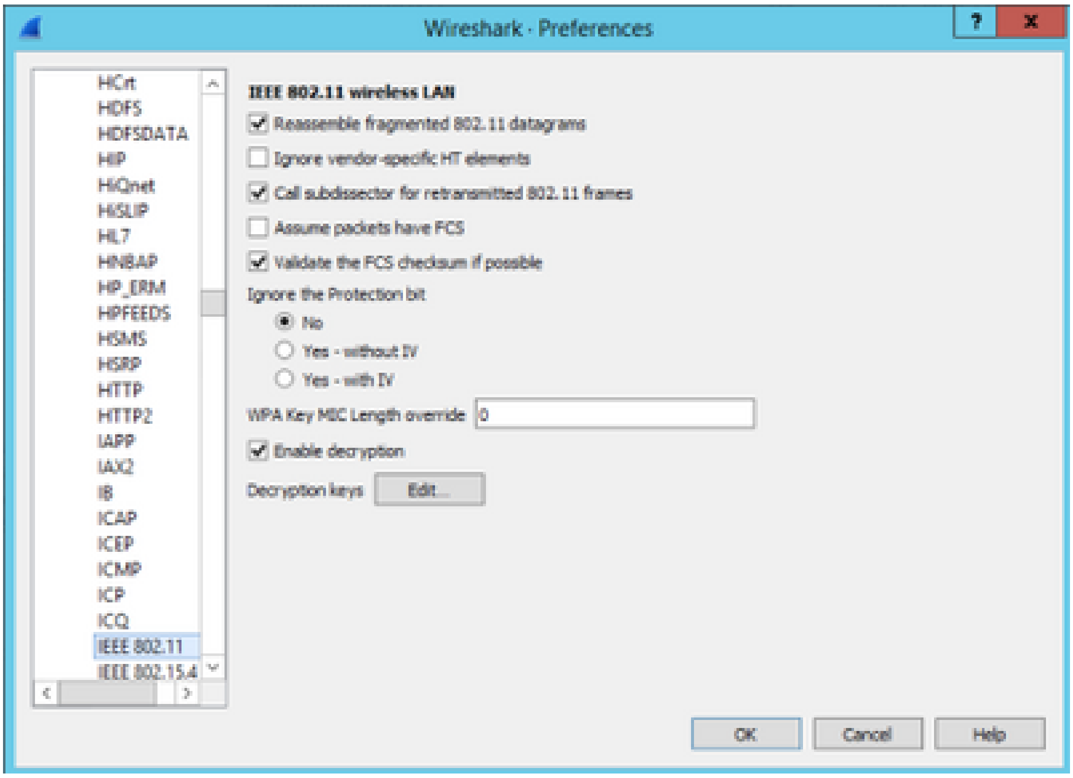
```
PMK:
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

```
PMK:
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e
```

步驟3.解密OTA監聽器。

導覽至**Wireshark > Preferences > Protocols > IEEE 802.11。然後勾選Enable Decryption**，然後按一下**Decryption Keys**旁邊的**Edit**按鈕，如下圖所示。



IEEE 802.11 wireless LAN

☑ Reassemble fragmented 802.11 datagrams

□ Ignore vendor-specific HT elements

☑ Call subdissector for retransmitted 802.11 frames

□ Assume packets have FCS

☑ Validate the FCS checksum if possible

Ignore the Protection bit

● No

○ Yes - without IV

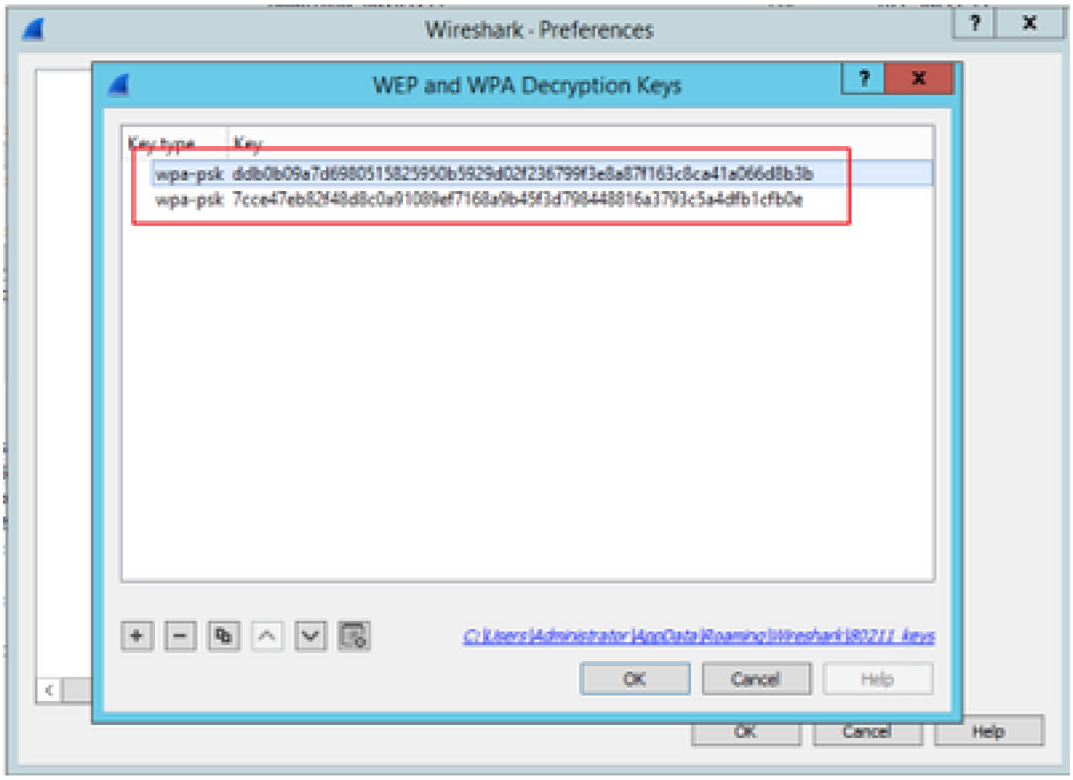
○ Yes - with IV

WPA Key MIC Length override: 0

☑ Enable decryption

Decryption keys: Edit...

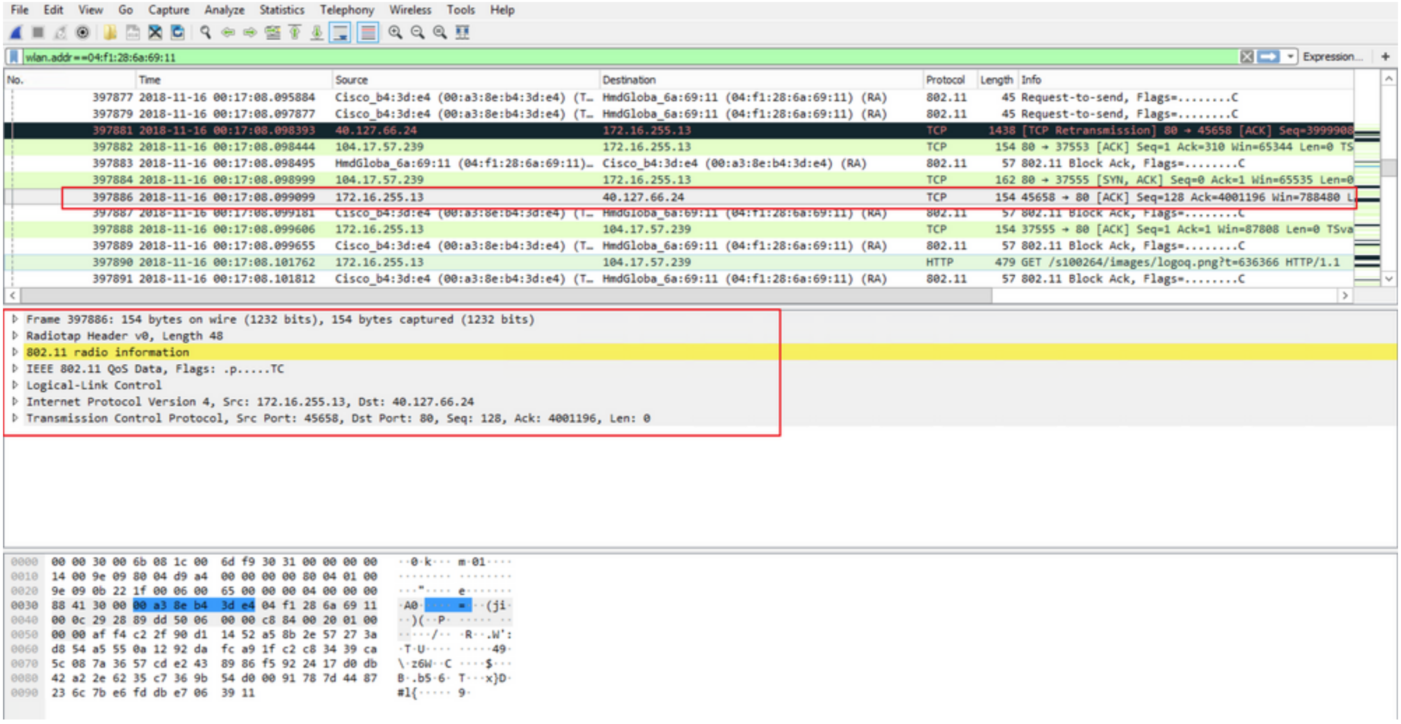
接下來，請選擇**wpa-psk**作為金鑰型別，並將派生的PMK放在**金鑰**欄位中，然後按一下**確定**。完成後，OTA捕獲應被解密，您會看到更高級別的層(3+)資訊。



Key type	Key
wpa-psk	ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
wpa-psk	7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

C:\Users\Administrator\AppData\Roaming\Wireshark\80211_keys

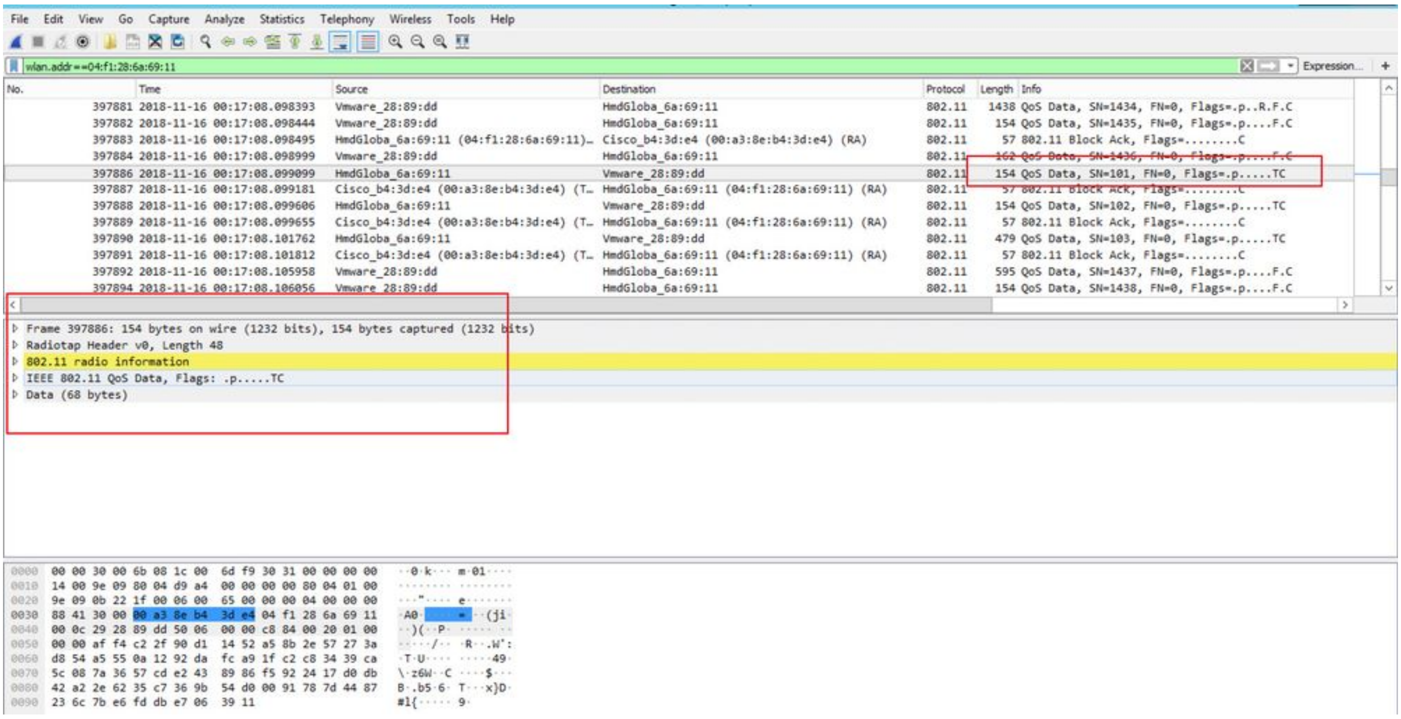
已解密的802.11資料包示例


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
wlan.addr==04:f1:28:6a:69:11

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/logoq.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 80 04 d9 a4  00 00 00 00 80 04 01 00   ················
0020  9e 09 0b 22 1f 00 06 00  65 00 00 00 04 00 00 00   ···"····e·······
0030  88 41 30 00 00 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   \·z6W··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·
```

如果比較未包括PMK的第二個結果與包括PMK的第一個結果，則資料包397886將解密為802.11 QoS資料。

加密的802.11資料包示例


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+

```
wlan.addr==04:f1:28:6a:69:11

No.     Time                        Source                                 Destination                                 Protocol Length Info
397881 2018-11-16 00:17:08.098393 Vmware_28:89:dd                         HmdGloba_6a:69:11                          802.11 1438 QoS Data, SN=1434, FN=0, Flags=.p..R.F.C
397882 2018-11-16 00:17:08.098444 Vmware_28:89:dd                         HmdGloba_6a:69:11                          802.11  154 QoS Data, SN=1435, FN=0, Flags=.p....F.C
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 Vmware_28:89:dd                         HmdGloba_6a:69:11                          802.11  162 QoS Data, SN=1436, FN=0, Flags=.p....F.C
397886 2018-11-16 00:17:08.099099 HmdGloba_6a:69:11                       Vmware_28:89:dd                            802.11  154 QoS Data, SN=101, FN=0, Flags=.p.....TC
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 HmdGloba_6a:69:11                       Vmware_28:89:dd                            802.11  154 QoS Data, SN=102, FN=0, Flags=.p.....TC
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 HmdGloba_6a:69:11                       Vmware_28:89:dd                            802.11  479 QoS Data, SN=103, FN=0, Flags=.p.....TC
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
397892 2018-11-16 00:17:08.105958 Vmware_28:89:dd                         HmdGloba_6a:69:11                          802.11  595 QoS Data, SN=1437, FN=0, Flags=.p....F.C
397894 2018-11-16 00:17:08.106056 Vmware_28:89:dd                         HmdGloba_6a:69:11                          802.11  154 QoS Data, SN=1438, FN=0, Flags=.p....F.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
▷ Data (68 bytes)

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 80 04 d9 a4  00 00 00 00 80 04 01 00   ················
0020  9e 09 0b 22 1f 00 06 00  65 00 00 00 04 00 00 00   ···"····e·······
0030  88 41 30 00 00 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   \·z6W··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·
```

注意：您可能會在解密時遇到Wireshark問題，在這種情況下，即使提供了正確的PMK（或者使用了PSK，也提供了SSID和PSK），Wireshark也不會解密OTA捕獲。因應措施是關閉Wireshark並開啟幾次，直到可以獲得更高層資訊並且802.11資料包不再顯示為QoS資料，或者使用安裝了Wireshark的另一台PC/Mac。

提示：名為pmkXtract的C++代碼附加在「相關資訊」中的第一個帖子中。已成功嘗試編譯並獲得執行檔，但可執行程式由於某些未知原因似乎未正確執行解密。此外，在第一篇帖子的評

論區域發佈了一個試圖提取PMK的Python指令碼，如果讀者感興趣，可以進一步研究該指令碼。

相關資訊

- **調整EAP的弱連結 — 使用pmkXtract從RADIUS中吸入WiFi PMK**
- **如何解碼Radius MS-MPPE-Recv-Key**
- **技術支援與文件 - Cisco Systems**