Configure o Wireshark e o FreeRADIUS para descriptografar o Sniffer sem fio 802.11 WPA2-Enterprise/EAP/dot1x over-the-air

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Procedimento Etapa 1. Descriptografar PMK(s) do pacote Access-accept. Etapa 2. Extraia PMK(s). Etapa 3. Descriptografar o Sniffer OTA. Exemplo de um pacote 802.11 descriptografado Exemplo de um pacote 802.11 criptografado Informações Relacionadas

Introduction

Este documento descreve como descriptografar o sniffer de Wi-Fi Protected Access 2 - Enterprise (WPA2-Enterprise) ou 802.1x (dot1x) criptografado sem fio por via aérea (OTA), com qualquer método EAP (Extensible Authentication Protocol).

Érelativamente fácil descriptografar a captura OTA 802.11 baseada em PSK/WPA2-Personal, desde que sejam capturados os handshakes EAPover LAN (EAPoL) completos de quatro vias. No entanto, a chave pré-compartilhada (PSK) nem sempre é recomendada do ponto de vista da segurança. Decifrar uma senha codificada é apenas uma questão de tempo.

Portanto, muitas empresas escolhem o dot1x com Remote Authentication Dial-In User Service (RADIUS) como uma melhor solução de segurança para sua rede sem fio.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- FreeRADIUS com o radsniff instalado
- Wireshark/Omnipeek ou qualquer software capaz de descriptografar o tráfego sem fio 802.11
- Privilégio de obter o segredo compartilhado entre o Network Access Server (NAS) e o Authenticator
- Capacidade de capturar a captura de pacote raio entre o NAS e o autenticador da primeira

solicitação de acesso (do NAS para o autenticador) para a última aceitação de acesso (do autenticador para o NAS) durante toda a sessão EAP

 Capacidade de executar captura OTA (Over-the-Air) contendo handshakes EAPoL de quatro vias

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Servidor Radius (FreeRADIUS ou ISE)
- Dispositivo de captura over-the-Air
- Apple macOS/OS X ou dispositivo 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Neste exemplo, duas PMKs (Pairwise Master Keys) são derivadas de pacotes Radius capturados do ISE 2.3, já que o tempo limite da sessão neste SSID é de 1800 segundos, e a captura fornecida aqui tem 34 minutos (2040 segundos).

Como mostrado na imagem, o EAP-PEAP é usado como exemplo, mas isso pode ser aplicado a qualquer autenticação sem fio baseada em dot1x.

| I. | wlan.ad | dr==04:f1:28:6a:69:11 && (eapol or eap) |) | | | | Expression | 4 |
|----|---------|---|-------------------|-------------------|----------|--------|--|-----|
| N | | Time | Source | Destination | Protocol | Length | Info | 1 |
| Т | 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) | _ |
| Ι | 4329 | 2018-11-16 00:04:02.816752 | Cisco_b4:3d:e4 | HmdGloba_6a:69:11 | EAP | 109 | Request, Protected EAP (EAP-PEAP) | |
| Τ | 4332 | 2018-11-16 00:04:02.818331 | HmdGloba_6a:69:11 | Cisco_b4:3d:e4 | TLSV1.2 | 244 | client Hello | - F |
| | 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 Hello | |
| I | 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 Hello | |
| | 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 | |
| 1 | 4367 | 2018-11-16 00:04:02.853063 | HmdGloba_6a:69:11 | Cisco_b4:3d:e4 | EAP | 73 | Response, Protected EAP (EAP-PEAP) | • |
| < | | | | | | | > | |

| | I d | (🖲) 🌡 🛅 🗙 🛅 9, 👄 🔿 | 🕾 🖲 🛓 📃 🔍 Q, Q, N | | | | |
|-----|---------|---|-------------------|-------------------|----------|--|---|
| | wlan.ad | dr==04:f1:28:6a:69:11 && (eapol or eap) |) | | | Expression | + |
| No. | | Time | Source | Destination | Protocol | Length Info | ^ |
| T | 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, En | |
| | 9895_ | 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 I | |
| | 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) | |
| T | 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 | 1 |
| | 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) | v |
| < | | | | | | 2 | |

Procedimento

Etapa 1. Descriptografar PMK(s) do pacote Access-accept.

Execute o **radsniff** contra a captura de raio entre o NAS e o Authenticator para extrair o PMK. A razão pela qual dois pacotes aceitos pelo acesso são extraídos durante a captura é que o temporizador de tempo limite da sessão é definido como 30 minutos neste SSID específico e a captura tem 34 minutos de duração. A autenticação é executada duas vezes.

```
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 = 0x52656175746853657373696f6e3a30613432346632613030303030303565373562656530393732
Class =
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 = 0x52656175746853657373696f6e3a306134323466326130303030303565373562656530393732
Class =
2f33303434
EAP-Message = 0x03910004
Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9
MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb
MS-MPPE-Recv-Key =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfblcfb0e<<<<<<<<PMK
Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

Note: Remova qualquer marca de LAN virtual (VLAN) da captura de pacote Radius; caso contrário, **radsniff** não reconhece o arquivo pcap de entrada. Para remover qualquer marca de VLAN, por exemplo, <u>editcap</u> pode ser usado.

Tip: Geralmente, o tempo de execução do comando **radsniff** em um arquivo pcap RADIUS pode ser contado como uma escala de segundos. No entanto, se o **radsniff** estiver preso nesse estado mostrado no registro, faça a cascata dessa captura de pacote (A) com outra

captura de pacote (B) mais longa entre o mesmo NAS e o mesmo Autenticador. Em seguida, execute o comando radsniff no pacote em cascata (A+B). O único requisito da captura de pacotes (B) é que você pode executar o comando radsniff contra ele e ver um resultado detalhado.

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)

Neste exemplo, o registro de plano de controle (A) do Wireless Lan Controller (WLC) capturado por meio do recurso de <u>registro de pacotes da WLC</u>, é em cascata com uma captura mais longa do TCPdump (B) do ISE. O registro de pacotes da WLC é usado como exemplo, porque geralmente é muito pequeno.

Registro de pacote (A) da WLC



Em seguida, execute o radsniff contra o pcap mesclado (A+B) e você poderá ver a saída verbosa.

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>

Etapa 2. Extraia PMK(s).

A exclusão de um campo 0x em cada **MS-MPPE-Recv-Key** da saída verbosa e os PMKs necessários para o decodificador de tráfego sem fio são então apresentados.

MS-MPPE-Chave-Recv = 0xdb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41c a066d8b3b

PMK:

ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d7984816a3793c5a4dfb1cc b0e

Etapa 3. Descriptografar o Sniffer OTA.

Navegue até Wireshark > Preferences > Protocols > IEEE 802.11. Em seguida, marque Enable Decryption (Ativar descriptografia) e clique no botão Edit (Editar) ao lado de Decryption Keys (Chaves de descriptografia), como mostrado na imagem.

| Wireshark · Preferences | ? | x |
|---|------|---|
| HCrt AC HDFS Reassemble fragmented 802.11 datagrams HDFSDATA Ignore vendor-specific HT elements HKQnet Call subdissector for retransmitted 802.11 frames HSLIP Assume packets have FCS HNBAP Validate the PCS checksum if possible HPFEEDS MS HSRP Ignore the Protection bit HYPE No Yes - without IV Yes - with IV HTTP WPA Key MCL Length override IAX2 B ICAP Decryption keys ICQ EEE 802.11 IEEE 802.15.4 X | Help | |

Em seguida, selecione **wpa-psk** como o tipo de chave, coloque os PMKs derivados no campo **Key** e clique em **OK**. Depois que isso for concluído, a captura OTA deverá ser descriptografada e você poderá ver informações da camada superior (3+).

| 4 | Wireshark - Preferences | ? X |
|---|--|------|
| | WEP and WPA Decryption Keys Y | |
| | Key type Key wpa-psk ddb0b09a7d6980515825950b5929d02/236799f3e8a87f163c8ca41a066d8b3b wpa-psk 7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e | |
| | | |
| | + - Pa A V B <u>C. Keers Holmistrator HooCata Roaming Wreehark (80211 Jens</u> OK Cancel Help | |
| | OK Cancel | Help |

Exemplo de um pacote 802.11 descriptografado

| File E | dit View Go Capture Analyze Statistics | Telephony Wireless Tools Help | | | | |
|--------|---|---|--|----------|--|---|
| | 1 🖲 🎍 🗅 🗙 🖨 🍳 👄 🕾 🗑 🜡 | k 🚍 🔳 @, @, @, II | | | | |
| wlan | addr = =04:f1:28:6a:69:11 | | | | Expression | + |
| No. | Time | Source | Destination | Protocol | Length Info | ^ |
| 1 | 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 | |
| 1 | 397881 2018-11-16 00:17:08.098393 | 40.127.66.24 | 172.16.255.13 | TCP | 1438 [TCP Retransmission] 80 → 45658 [ACK] Seg=3999908 | _ |
| | 397882 2018-11-16 00:17:08.098444 | 104.17.57.239 | 172.16.255.13 | TCP | 154 80 → 37553 [ACK] Seg=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] Seg=128 Ack=4001196 Win=788480 L | |
| | 397887 2018-11-16 00:17:08.099181 | Cisco_b4:3d:e4 (00:a3:8e:b4:3d:e4) (1_ | HmdGloba_6a:69:11 (04:11:28:6a: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 | |
| < | | | | | > | |
| b Ena | me 397886: 154 hytes on wine (1232 hits) | 154 butes cantured (1232 bits) | | | | |
| b Rad | ictan Header v@ Length 48 | , 154 bytes captured (1252 bits) | | | | |
| b 882 | 11 radio information | | | | | |
| D TEE | F 802.11 OoS Data, Flags: .nTC | | | | | |
| D Log | ical-Link Control | | | | | |
| D Int | ernet Protocol Version 4. Sec: 172.16.255 | 5.13. Dst: 40.127.66.24 | | | | |
| P Tra | nsmission Control Protocol, Src Port: 456 | 658. Dst Port: 80. Seg: 128. Ack: 400119 | . Len: 0 | | | |
| | | | ,, | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| 0000 | 00 00 30 00 6b 08 1c 00 6d f9 30 31 00 | 00 00 00 ··O·k··· m·01···· | | | | |
| 0010 | 14 00 9e 09 80 04 d9 a4 00 00 00 00 80 | 04 01 00 | | | | |
| 0020 | 98 09 00 22 IT 00 00 00 05 00 00 00 04 | 6a 60 11 .40. e | | | | |
| 0030 | 88 41 58 68 68 68 68 64 50 64 11 28 | 20 01 00 ···)(··P····· | | | | |
| 0050 | 00 00 af f4 c2 2f 90 d1 14 52 a5 8b 2e | 57 27 3a ·····/·· · · ······················· | | | | |
| 0060 | d8 54 a5 55 0a 12 92 da fc a9 1f c2 c8 | 34 39 ca .T.U | | | | |
| 0070 | 5c 08 7a 36 57 cd e2 43 89 86 f5 92 24 | 17 d0 db \.z6WC\$ | | | | |
| 0080 | 42 a2 2e 62 35 c7 36 9b 54 d0 00 91 78 | 7d 44 87 Bb5.6. Tx}D. | | | | |
| 0090 | 23 6c 7b e6 fd db e7 06 39 11 | #1{9. | | | | |

Se você comparar o segundo resultado em que o PMK não está incluído, com o primeiro resultado, em que o PMK está incluído, o pacote 397886 é descriptografado como dados de QoS 802.11.

Exemplo de um pacote 802.11 criptografado

| addr | =04:f1:28:6a:69:11 | | | | 🛛 🗔 🔹 E |
|--|--|---|--|----------|---|
| | 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=.pR.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=.pF.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, FlagspF.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=.pTC |
| | 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= |
| | 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=.pTC |
| | 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=.pTC |
| | 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=.pF.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=.pF.C |
| | | | | | |
| 802.11 IEEE 80 Data (6 | adio information 2.11 QoS Data, Flags: .pTC 3 bytes) | | | | |
| 802.11 IEEE 80 Data (6 | adio information 2.11 QoS Data, Flags: .pTC 5 bytes) | | | | |
| 802.11 IEEE 80 Data (6 | adio information 111 QoS Data, Flags: .pTC bytes) | | | | |
| 802.11 IEEE 80 Data (6 | adio information .11 QoS Data, Flags: .pTC bytes) | | | | |
| 802.11 IEEE 80 Data (6 | adio information .11 QoS Data, Flags: .pTC i bytes) | | | | |
| 802.11 IEEE 80 Data (6 | adio information .11 QoS Data, Flags: .pTC bytes) | | | | |
| 802.11 IEEE 80 Data (6 | adio information .11 QoS Data, Flags: .pTC i bytes) 0 30 00 65 08 1c 00 6d f9 30 31 00 | 90 00 00 ····· m··01···· | | | |
| 802.11 IEEE 80 Data (6 Data (6 00 00 (1 10 14 (1 | adio information .11 QoS Data, Flags: .pTC i bytes) 0 30 00 65 08 1c 00 6d f9 30 31 00 0 92 09 20 80 4d 9a 4 00 00 00 80 | 90 00 00 ······························ | | | |
| 802.11 IEEE 80 Data (6 Data (6 0 00 0 10 14 (20 9e (| e 30 00 65 00 12 00 64 f9 30 31 00 0 90 00 65 00 12 00 64 f9 30 31 00 0 90 09 66 00 12 00 64 f9 30 31 00 0 90 09 80 04 99 4 00 00 00 80 9 00 22 11 00 06 00 65 80 00 00 40 | 00 00 00 -0:k m.01 | | | |
| 802.11 IEEE 80 Data (6 00 00 (18 14 (20 9e (30 88 4 | adio information .11 QoS Data, Flags: .pTC i bytes) 0 30 00 6b 08 1c 00 6d f9 30 31 00 0 9e 09 20 6d d9 ad 00 00 00 80 9 0b 22 1f 00 66 00 65 00 00 00 41 130 00 00 00 ad 0e bid 3d ed 04 f1 28 - 00 00 00 00 ad 0e bid 3d ed 04 f1 28 | 00 00 00 · · 0 · k · · · m · 01 · · · · 04 01 00 00 00 · · · · · · · e · · · · · 6 00 00 00 · · · · · · · e · · · · · · 6 00 11 · · · A0; • • · · · (j1 | | | |
| 802.11 IEEE 80 Data (6) 00 00 (10 14 (20 9c (30 88 4 40 00 (| adio information | 00 00 00 0 • 0 k • m • 01 • • • • • • • • • • • • • • • • • | | | |
| 802.11 IEEE 80 Data (6) 000 00 0 018 14 0 020 9e 0 030 88 4 040 00 0 050 00 0 | adio information .11 QoS Data, Flags: .pTC i bytes) 0 30 00 6b 08 1c 00 6d f9 30 31 00 0 9e 98 06 4d9 a4 00 00 00 00 80 9 bb 22 1f 00 66 00 58 00 00 00 04 1 30 00 00 80 33 56 b4 3d ce 04 f1 28 c 29 28 80 4d 59 a6 00 0e 00 e8 04 0 a6 50 a1 56 b4 3d ce 04 f1 28 c 29 28 80 4d 59 a6 00 0e 00 e8 84 0 a6 f4 c2 2f 90 d1 14 52 a5 5b 2e 4 4 a5 55 0a 12 29 2d af ca 91 4r 2 a8 | 60 60 60 ···0·k··· m·01···· 64 61 60 64 61 60 66 69 11 ···0· 62 01 00 ····(j1 20 100 ···)(··P····· 57 27 3a ····/· 8···¥': 49 ···· | | | |
| 802.11 IEE 80 Data (6 815 14 (828 94 838 84 846 00 (858 00 (856 00 (850 | adio information | 00 00 00 · · 0·k··· m·01···· 04 01 00 · · · · · · · · · · · · · · · · · | | | |
| 802.11 IEEE 80 Data (6 018 14 (220 9c (338 84 040 00 (50 00 (50 00 (50 00 (50 00 (50 00 (50 0 (50 0) (50 0 (50 0) (50 0 (50 0 (50 0) (50 0 (50 0 (50 0 (50 0) (50 0 (50 0) (50 0 (50 0 (50 0) (50 0 | adio information | 00 00 00 · · 0 · k · · · m · 01 · · · · · · · · · · · · · · · · · | | | |

Caution: Você pode encontrar um problema com o Wireshark na descriptografia e, nesse caso, mesmo se o PMK correto for fornecido (ou se a PSK for usada, o SSID e a PSK forem fornecidos), o Wireshark não descriptografa a captura OTA. A solução alternativa é desligar o Wireshark e ligá-lo algumas vezes até que as informações da camada mais alta possam ser obtidas e os pacotes 802.11 não sejam mais mostrados como dados de QoS, ou usar

outro PC/Mac onde o Wireshark está instalado.

Dica: um código C++ chamado pmkXtract está anexado à primeira publicação em Informações Relacionadas. As tentativas de compilação foram bem-sucedidas e um arquivo executável é obtido, mas o programa executável não parece executar a descriptografia corretamente por alguns motivos desconhecidos. Além disso, um script Python que tenta extrair PMK é publicado na área de comentários da primeira publicação, que pode ser explorada se os leitores estiverem interessados.

Informações Relacionadas

- Ajustando o link fraco do EAP extraindo PMKs Wi-Fi do RADIUS com pmkXtract
- Como decodificar MS-MPPE-Recv-Key RADIUS
- Suporte Técnico e Documentação Cisco Systems