配置Wireshark和FreeRADIUS以解密802.11 WPA2-Enterprise/EAP/dot1x over-the-air无线嗅 探器

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> <u>使用的组件</u> <u>背景信息</u> <u>步骤</u> <u>步骤1.从Access-accept数据包解密PMK。</u> <u>步骤2.提取PMK。</u> <u>步骤3.解密OTA嗅探器。</u> <u>解密的802.11数据包示例</u> 加密802.11数据包示例 相关信息

简介

本文档介绍如何使用任何可扩展身份验证协议(EAP)方法解密Wi-Fi保护访问2 — 企业版(WPA2-Enterprise)或802.1x(dot1x)加密无线空中(OTA)嗅探器。

只要捕获完整的四路EAP over LAN(EAPoL)握手,就相对容易解密基于PSK/WPA2-personal 802.11 OTA捕获。但是,从安全角度来看,并不总是建议使用预共享密钥(PSK)。破解硬编码密码 只是时间问题。

因此,许多企业选择带有远程身份验证拨入用户服务(RADIUS)的dot1x作为其无线网络的更好的安全解决方案。

先决条件

要求

Cisco 建议您了解以下主题:

- 安装了radsniff的FreeRADIUS
- Wireshark/Omnipeek或任何能够解密802.11无线流量的软件
- 在网络访问服务器(NAS)和验证器之间获取共享密钥的权限
- 能够在整个EAP会话中捕获NAS和身份验证器之间的RADIUS数据包捕获,从第一个访问请求 (从NAS到身份验证器)到最后一个访问接受(从身份验证器到NAS)
- •能够执行包含四路EAPoL握手的空中(OTA)捕获

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Radius服务器(FreeRADIUS或ISE)
- 空中捕获设备
- Apple macOS/OS X或Linux设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

在本示例中,两个成对主密钥(PMK)从从ISE 2.3捕获的Radius数据包派生,因为此SSID的会话超时 为1800秒,此处提供的捕获为34分钟(2040秒)。

如图所示,EAP-PEAP用作示例,但可以应用于任何基于dot1x的无线身份验证。

	wlan.addr==04:f1:28:6a:69:11 && (eapol or eap)			Expression	•
No	o. Time	Source	Destination	Protocol Length Info		Ī
Т	4325 2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, TLS EAP (EAP-TLS)		I
	4327 2018-11-16 00:04:02.812927	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Legacy Nak (Response Only)		ł
	4329 2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP 109 Request, Protected EAP (EAP-PEAP)		I
T	4332 2018-11-16 00:04:02.818331	HmdGloba_6a:69:11	Cisco_b4:3d:e4	ILSVI.2 244 Client Hello		ŀ
	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	I
T	4352 2018-11-16 00:04:02.829281	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)		I
T	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	I
	4356 2018-11-16 00:04:02.834110	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)		I
	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	I
	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, Encry	ted Handshak	I
	4365 2018-11-16 00:04:02.851843	Cisco_b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2 124 Change Cipher Spec, Encrypted Handshake Messag		L
	4367 2018-11-16 00:04:02.853063	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP 73 Response, Protected EAP (EAP-PEAP)		1
¢						

1		. 🖲 🕌 🖾 🗙 🖾 🤇 🐡 🤝	열 🛚 👲 📃 📃 약, 약, 약, 표					
	wlan.ad	dr==04:f1:28:6a:69:11 && (eapol or eap))			🔀 📼 🔹 Expression.	. +	
N	o.	Time	Source	Destination	Protocol	Length Info	^	ŝ
Τ	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		
Ι	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		
1	9095	2018-11-16 00:34:07.525423	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89 Response, Protected EAP (EAP-PEAP)		
Т	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		
	9895_	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	() ka	i
	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		
	9895_	2018-11-16 00:34:07.575693	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89 Response, Protected EAP (EAP-PEAP)	V	í
-								

步骤

步骤1.从Access-accept数据包解密PMK。

在NAS和身份验证器之间针对RADIUS捕获运行**radsniff**以提取PMK。捕获期间提取两个accessaccept数据包的原因是,会话超时计时器在此特定SSID上设置为30分钟,捕获时间为34分钟。身份 验证执行两次。

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 = 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 =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e<<<<<<<<<<PMK
Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

注意:请删除Radius数据包捕获的任何虚拟LAN(VLAN)标记,否则,**radsniff**无法识别输入 pcap文件。例如,要删除任何VLAN标记,可<u>使用editcap</u>。

提示:通常,针对RADIUS pcap文件的**radsniff**命令的运行时可以计为秒级。但是,如果 radsniff陷入日志中显示的此状态,请将此数据包捕获(A)与同一NAS和身份验证器之间的另一 个较长数据包捕获(B)级联。然后,对级联数据包(A+B)运行radsniff命令。数据包捕获(B)的唯 一要求是您能够针对它运行radsniff命令并查看详细结果。

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius_novlan.pcap -s Ciscol23 -x

Logging all events

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

在本示例中,通过<u>WLC数据包日志记录功能捕获的无线局域网控制器(</u>WLC)控制平面日志记录(A)与 从ISE的TCPdump(B)捕获的更长捕获相级联。WLC数据包日志记录作为示例,因为其大小通常非 常小。

WLC数据包日志记录(A)

📾 radius novlan.pcap	Pcap Napture	22 KB	Today a	at 11:56 am	
			,		
ISE Tcpdump(B)					
📓 radius_eap_decode_Cisco123.pcap	Yesterday at 12:04 pm	Ę	350 KB	Pcap Napture	

Pcapn...Capture

927 KB Today at 12:28 pm

🔚 radius_novlan_merged.pcapng

然后对合并的pcap(A+B)运行radsniff,您将能够看到详细输出。

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>

步骤2.提取PMK。

然后,从详细输出中删除每个MS-MPPE-Recv-Key中的0x字段,并显示无线流量解码所需的PMK。

MS-MPPE-Recv-Key = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

рмк: ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

PMK:

 $7 \verb+cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfblcfb0e$

步骤3.解密OTA嗅探器。

导航至Wireshark > Preferences > Protocols > IEEE 802.11。**然后,选中**Enable Decryption,然后 单击Decryption Keys旁边的Edit按钮,如图所示。

A	Wireshark - Preferences ?	x
HCrt A HDFS HDFSDATA HP HQnet HSLIP HL7 HNBAP HP_ERM HPFEEDS HSMS HSRP HTTP HTTP2 IAV2 IB ICAP ICAP ICAP ICC ICC IEEE 802.11 IEEE 802.11	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 Decryption keys Edit	

接下来,请选**择wpa-psk**作为密钥类型,将派生的PMK放在**Key**字段中,然后单击**OK**。完成此操作 后,应解密OTA捕获,您可以看到更高的层(3+)信息。

		Wireshark - Prefere	inces		?	x
	🛋 W	EP and WPA Decrypti	on Keys	? ×	1	
	Key Key wpa-psk ddb0b09a7d69805155 wpa-psk 7cce47eb82f48d8c0af + = • •	25950b5929d02f236799f3e 1089ef7168a9b45f3d79844 C: Kters J4dministra	8#87#163c8c#41#066d8b38 8816#3793c5#4dfb1cfb0e tor:j4coCata Koaming litting			
¢			OK Cancel	Help	Help	
			OK	Cancel	He	p

解密的802.11数据包示例

File Edit	View Go Capture Analyze Statistics T	elephony Wireless Tools Help			
	ا 🗿 🔛 🗠 🗢 🛸 🛣 🚵	📜 📃 Q, Q, Q, 🔢			
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] 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) (1_	HmdGloba_6a:69:11 (04:†1:28:6a:69:11) (RA)	802.11	5/ 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
i	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 39	7886: 154 bytes on wire (1232 bits),	154 bytes captured (1232 bits)			
Radiotap	Header v0, Length 48				
Þ 802.11 r	adio information				
IEEE 802	.11 QoS Data, Flags: .pTC				
Logical-	Link Control				
Internet	Protocol Version 4, Src: 172.16.255	.13, Dst: 40.127.66.24			
Transmis	sion Control Protocol, Src Port: 456	58, Dst Port: 80, Seq: 128, Ack: 4001196	, Len: 0		
0000 00 0	0 30 00 6b 08 1c 00 6d f9 30 31 00 0	00 00 00 ··0·k··· m·01····			
0010 14 0	0 9e 09 80 04 d9 a4 00 00 00 80 0	84 81 88			
0020 9e 0	9 0b 22 1f 00 06 00 65 00 00 00 04 0	00 00 00 ····"···· e·····			
0030 88 4	1 30 00 00 a3 8e b4 3d e4 04 f1 28 0	5a 69 11 · A0· · (ji·			
0040 00 0	c 29 28 89 dd 50 06 00 00 c8 84 00 2	20 01 00 ··)(··P······			
0000 0000	0 at t4 c2 2t 90 d1 14 52 a5 60 2e 3	2/ 20 ca . T.II			
0070 5c 0	8 7a 36 57 cd e2 43 89 86 f5 92 24 1	17 d0 db \.z6WC\$			
0080 42 a	2 2e 62 35 c7 36 9b 54 d0 00 91 78 7	7d 44 87 Bb5.6. Tx}D.			
0090 23 6	c 7b e6 fd db e7 06 39 11	#1{9.			

如果将未包含PMK的第二个结果与包含PMK的第一个结果进行比较,则数据包397886将解密为802.11 QoS数据。

加密802.11数据包示例

PTHON 1 (0),	dr==04:f1:28:6a:69:11				Expres
	Time	Source	Destination	Protocol	Length Info
	307881 2018-11-16 00-17-08 008303	Versage 28-80-dd	Hedőloba 6a:60:11	802 11	1438 OoS Data SN=1434 EN=0 Elags= o D E C
	397882 2018-11-16 00-17-08 098444	Viniare 28:89:dd	HedGloba 6a:69:11	892 11	154 Ons Data SN=1435 EN=0 Flags= n E C
	307883 2018-11-16 00:17:08 008495	HerdGloba 6a:60:11 (04:f1:28:6a:60:11)	(isco h4:3dre4 (00:s3:8e;h4:3dre4) (04)	802 11	57 892 11 Block Ack Elagra
	397884 2018-11-16 00:17:08 008999	Vmcare 28:89:dd	HedGloba 6a:69:11	802 11-	162 Oct. Date CN 1436 CN 0 Flore
	307886 2018-11-16 00-17-08 000000	HedGloba 6a:60:11	Vewage 28:80:dd	802 11	154 OoS Data SN=101 EN=0 Elage= n TC
	397887 2018-11-16 00:17:08.099181	Cisco b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdG]cha_6a:69:11 (04:f1:28:6a:69:11) (84)	802.11	5/ 80/.11 Block ack. Flags
	397888 2018-11-16 00:17:08 099505	HedGloba 6a:69:11	Veware 28:89:dd	892.11	154 OoS Data SN=102 EN=0 Flags= 0 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) (84)	802.11	57 892.11 Block Ack, Flags
	397890 2018-11-16 00:17:08.101762	HendGloba 6a:69:11	Vmware 28:89:dd	802.11	479 0oS 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) (84)	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 OoS Data, SN=1437, FN=0, Flags=, pF.C
	397894 2018-11-16 00:17:08,106056	Vmware 28:89:dd	HedGloba 6a:69:11	802.11	154 OoS Data, SN=1438, FN=0, Flags=, p, F.C
Data	(68 bytes)				
lata	(68 bytes)				
ata	(68 bytes)				
ata	(68 bytes)				
ata	(68 bytes)				
)ata	(68 bytes)				
)ata	(68 bytes)				
ata	(68 bytes) 9 00 30 00 6b 08 1c 00 6d f9 30 31 00	00 00 00 ···0·k···· m·01····			
Data Data	(68 bytes) 9 00 30 00 6b 08 1c 00 6d f9 30 31 00 6 00 9e 09 80 04 d9 a4 00 00 00 80	00 00 00 ···0·k··· m·01···· 04 01 00			
Data 00 00 10 10 20 90	(68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 10 09 09 23 00 04 09 a4 00 00 00 00 09 09 25 21 00 06 00 00 00	00 00 00 ···0·k··· m·01···· 04 01 00 ···· ··· e ·····			
Data 30 04 18 14 28 94 38 85	(68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 1 00 9c 03 80 04 69 a4 00 00 00 60 09 0b 22 1f 00 66 00 65 00 00 00 04 41 30 00 00 00 a5 6e D4 30 04 04 04 12 28	00 00 00 ···0·k··· m·01···· 94 01 00 ···· 00 00 00 ···· ··· c···· 66 00 11 ·A0 ····· (ji			
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	(68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 6 00 9e 09 80 04 d9 a4 00 00 00 80 10 90 b 22 1f 00 06 00 65 00 00 04 41 30 00 00 03 0e 64 3d a4 04 f1 28 0 c 29 28 89 dd 50 06 00 00 c8 84 00	00 00 00 00 00 00 00 00 00 00 00 00 00			
Data 00 00 10 1 20 9 30 8 40 00 50 00	(68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 10 09 09 20 80 04 d9 a4 00 00 00 08 50 09 0b 22 16 00 65 20 00 00 43 41 30 00 00 a3 6b 43 3d e4 4f 12 35 0 6c 29 28 30 d5 90 60 00 06 84 00 10 02 f4 c2 2f 90 d1 14 52 a5 8b 2c	00 00 00 ···0·k···m·01···· 04 01 00 00 00 00 ····· e 6a 69 11 ·A0· •···(j1- 20 01 00 ····· 57 27 3a ····/··········			
Data 000 00 100 10 200 90 300 80 440 00 500 00000000	(68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 0 09 9c 09 30 04 d9 a4 00 00 00 00 80 09 0b 22 1f 00 06 00 65 00 00 00 41 41 30 00 00 a 3 be b4 3d e4 04 f1 28 0 c 29 28 89 d5 80 66 00 00 c8 84 00 00 af f c 2 2 f 90 d1 14 52 a5 8b 2e 5 4 a5 55 0a 12 92 da fc 91 fc 2c 68 08 7a 35 7c dc 24 39 26 f5 92 24	00 00 00 · 0 k · m 01 · · · · · · · · · · · · · · · · · ·			
Data 000 00 100 10 200 90 300 80 440 00 500 00000000	(68 bytes) 0 00 30 00 6b 08 1c 00 6d f9 30 31 00 0 09 09 20 00 4d 9 a4 00 00 00 08 09 09 22 16 00 65 00 00 00 08 41 30 00 00 a3 6e 54 3d e4 04 f3 28 0 c 29 28 9 d5 20 60 00 00 c8 84 00 00 a7 f4 c2 2f 90 d1 14 52 a5 8b 2e 54 a5 50 c4 22 43 89 86 f5 92 24 28 22 62 53 c7 36 95 44 00 91 78	00 00 00 k··· m·01···· 04 01 00 ···· 06 00 00 ···· 05 05 11 ·A0 ···· 05 05 11 ···· ···· 07 07 33 ····· ···· 77 27 33 ····· ···· 17 40 ···· ···· ×10 74 87 ···· ×10 ····			

警告:在解密时,您可能会遇到Wireshark的问题,在这种情况下,即使提供了正确的 PMK(或者使用了PSK,同时提供了SSID和PSK),Wireshark也不会解密OTA捕获。解决方 法是关闭Wireshark并打开几次,直到获得更高层信息,802.11数据包不再显示为QoS数据 ,或使用安装了Wireshark的另一台PC/Mac。

提示:在"相关信息"(Related Information)中的第一个帖子中附加了名为pmkXtract的C++代码 。已成功尝试编译并获取可执行文件,但由于某些未知原因,可执行程序似乎未正确执行解密 。此外,尝试提取PMK的Python脚本会发布在第一篇帖子的评论区,如果读者感兴趣,可以 进一步探讨该脚本。

相关信息

- 调整EAP的弱链路 使用pmkXtract从RADIUS中吸收WiFi PMK
- 如何解码Radius MS-MPPE-Recv-Key
- <u>技术支持和文档 Cisco Systems</u>