# 802.11 WPA2-Enterprise/EAP/dot1x over-the-air 무선 스니퍼를 해독하려면 Wireshark 및 FreeRADIUS를 구성합니다.

## 목차

소개 사전 요구 사항 요구 사항 사용되는 구성 요소 배경 정보 절차 1단계. Access-accept Packet에서 PMK를 해독합니다. 2단계. PMK를 추출합니다. 3단계. OTA 스니퍼를 해독합니다. 해독된 802.11 패킷의 예 암호화된 802.11 패킷의 예 관련 정보

### 소개

이 문서에서는 EAP(Extensible Sniffer Authentication Protocol) 방법을 사용하여 Wi-Fi Protected Access 2 - Enterprise(WPA2-Enterprise) 또는 802.1x(dot1x) 암호화된 OTA(Wireless over-the-air)를 해독하는 방법에 대해 설명합니다.

EAPoL(Full 4-Way EAP over LAN) 핸드쉐이크가 캡처되는 한 PSK 기반/WPA2-개인 802.11 OTA 캡처를 비교적 쉽게 해독할 수 있습니다.그러나 보안 관점에서 PSK(Pre-shared Key)가 반드시 권 장되지는 않습니다.하드코딩된 비밀번호를 깨는것은 시간문제일 뿐이다.

따라서 많은 기업에서 무선 네트워크를 위한 더 나은 보안 솔루션으로 원격 인증 전화 접속 사용자 서비스(RADIUS)가 있는 dot1x를 선택합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Radsniff가 설치된 FreeRADIUS
- Wireshark/Omnpeek 또는 802.11 무선 트래픽을 해독할 수 있는 모든 소프트웨어
- 네트워크 액세스 서버(NAS)와 인증자 간 공유 암호를 얻을 수 있는 권한
- EAP 세션 전체에서 첫 번째 액세스 요청(NAS에서 인증자에게)부터 마지막 액세스 수락(인증 자에서 NAS로)까지 NAS와 인증자 간에 RADIUS 패킷 캡처를 캡처하는 기능
- 4방향 EAPoL 핸드셰이크를 포함하는 OTA(Over-the-Air) 캡처 수행 능력

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Radius 서버(FreeRADIUS 또는 ISE)
- Over-the-Air 캡처 장치
- Apple macOS/OS X 또는 Linux 디바이스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

### 배경 정보

이 예에서 두 개의 PMK(Pairwise Master Keys)는 ISE 2.3에서 캡처된 Radius 패킷에서 파생됩니다. 이 SSID의 세션 시간 초과는 1800초이고 여기에 제공된 캡처는 34분(2040초)입니다.

이미지에 표시된 대로 EAP-PEAP가 예제로 사용되지만, 이는 모든 dot1x 기반 무선 인증에 적용할 수 있습니다.

wlan.	addr==04:f1:28:6a:69:11 && (eapol or eap	)			🔀 🔜 💌 Expressi	an
No.	Time	Source	Destination	Protocol	Length Info	
43	25 2018-11-16 00:04:02.812197	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP	109 Request, TLS EAP (EAP-TLS)	
43	27 2018-11-16 00:04:02.812927	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Legacy Nak (Response Only)	
43	29 2018-11-16 00:04:02.816752	Cisco_b4:3d:e4	HmdGloba_6a:69:11	EAP	109 Request, Protected EAP (EAP-PEAP)	
43	32 2018-11-16 00:04:02.818331	HmdGloba_6a:69:11	Cisco_b4:3d:e4	TLSV1.2	244 Client Hello	1
43	49 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 Hel	1
43	52 2018-11-16 00:04:02.829281	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Protected EAP (EAP-PEAP)	
43	54 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 Hel	1
43	56 2018-11-16 00:04:02.834110	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Protected EAP (EAP-PEAP)	
43	51 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 Hel	1
43	53 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 Handsha	k
43	55 2018-11-16 00:04:02.851843	Cisco b4:3d:e4	HmdGloba_6a:69:11	TLSv1.2	124 Change Cipher Spec, Encrypted Handshake Message	
43	57 2018-11-16 00:04:02.853063	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	73 Response, Protected EAP (EAP-PEAP)	
ć.						2
	al 📵 🔒 🗁 🗙 🔁 🔍 👄 👄	S T & S = Q Q Q W				

	wlan.add	dr==04:f1:28:6a:69:11 && (eapol or eap)	)				Expression	.   ·	÷
N	io.	Time	Source	Destination	Protocol	Length	Info		^
1	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 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		
П	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		
	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	1	in the
	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	( I	7
	9095_	2018-11-16 00:34:07.575693	HmdGloba_6a:69:11	Cisco_b4:3d:e4	EAP	89	Response, Protected EAP (EAP-PEAP)		v
1					_		2		

## 절차

### 1단계. Access-accept Packet에서 PMK를 해독합니다.

PMK를 **추출하려면** NAS와 인증자 간의 RADIUS 캡처에 대해 radsniff를 실행합니다.캡처 중에 두 개의 액세스 수락 패킷이 추출되는 이유는 세션 시간 초과 타이머가 이 특정 SSID에서 30분으로 설 정되고 캡처가 34분이기 때문입니다.인증은 두 번 수행됩니다.

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius\_novlan\_merged.pcapng s <shared-secret between NAS and Authenticator> -x

<snip>

```
+0.000
User-Name = "frlu_2"
State = 0x52656175746853657373696f6e3a30613432346632613030303030303565373562656530393732
Class =
2£33303432
EAP-Message = 0x03c50004
Message-Authenticator = 0x38c67b9ba349842c9624889a45cabdfb
MS-MPPE-Send-Key = 0xa464cc15c0df8f09edc249c28711eb13a6db2d1a176f1196edcc707579fd6793
MS-MPPE-Recv-Key =
0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b<<<<<<<<<<
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-Kev =
0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e<<<<<<<<<<<
Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
    참고:RADIUS 패킷 캡처의 가상 LAN(VLAN) 태그를 제거하십시오. 그렇지 않으면 radsniff에
    서 입력 pcap 파일을 인식하지 못합니다.예를 들어, VLAN 태그를 제거하려면 editcap을 사용
```

할 수 있습니다.

팁:일반적으로 RADIUS pcap 파일에 대한 radsniff 명령의 런타임을 초 단위로 계산할 수 있습 니다.그러나 radsniff가 로그에 표시된 이 상태에 머물러 있는 경우 동일한 NAS와 인증자 간에 이 패킷 캡처(A)를 더 긴 패킷 캡처(B)와 함께 전달하십시오.그런 다음 종속 연결된 패킷 (A+B)에 대해 radsniff 명령을 실행합니다. 패킷 캡처(B)의 유일한 요구 사항은 radsniff 명령을 실행하고 자세한 결과를 볼 수 있다는 것입니다.

FRLU-M-51X5:pcaps frlu\$ radsniff -I /Users/frlu/Downloads/radius\_novlan.pcap -s Cisco123 -x

Sniffing on (/Users/frlu/Downloads/radius\_novlan.pcap)

이 예에서 WLC 패킷 로깅 기능을 통해 캡처된 WLC(Wireless Lan Controller) 컨트롤 플레인 로깅 (A)은 ISE의 TCPdump(B)에서 더 긴 캡처를 통해 캐스케이드됩니다.WLC 패킷 로깅은 일반적으로 크기가 매우 작기 때문에 예시로 사용됩니다.

#### WLC 패킷 로깅(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		850 KB	Pcap Napture
- 병합됨(A+B)				
🔚 radius_novlan_merged.pcapng	PcapnCapture	927 KB	Today at	12:28 pm

그런 다음 병합된 pcap(A+B)에 대해 radsniff를 실행하면 자세한 출력을 볼 수 있습니다.

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>

### 2단계. PMK를 추출합니다.

자세한 정보 출력에서 각 **MS-MPPE-Recv-Key**의 0x 필드를 삭제하고 무선 트래픽 디코딩에 필요한 PMK를 표시합니다.

MS-MPPE-Recv-Key = 0xddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca4066d8b3b

PMK:

ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b

MS-MPPE-Recv-Key =

0x7cce47eb82f48d8c0a91089ef7168a9b45f3d7984816a3793c5a4dfb1cfb0e

PMK:

7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

### 3단계. OTA 스니퍼를 해독합니다.

Wireshark > **Preferences** > **Protocols** > **IEEE 802.11로** 이동한 다음 **Enable Decryption(암호 해독 활성화)**을 선택하고 이미지에 표시된 것처럼 Decryption Keys(암호 해독 키) 옆의 Edit(수정) 버튼을 클릭합니다.

4	Wireshark · Preferences ? X
HCrt HDFS HDFSDATA HP HiQnet HISUP HL7 HNBAP HP_ERM HPFEEDS HSMS HSRP HTTP HTTP2 IAPP IAX2 IB ICAP ICAP ICEP ICCP ICC ICP ICQ IEEE 802.11 IEEE 802.15,4	IHE 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 - with DV         WPA Key MIC Length override         Decryption keys
	OK Cancel Help

다음으로 **wpa-psk를** 키 유형으로 선택하고 **키** 필드에 파생된 PMK를 입력한 다음 **확인**을 **클릭합니 다**.이 작업이 완료되면 OTA 캡처의 암호를 해독해야 하며 상위 계층(3+) 정보를 볼 수 있습니다.

	Wireshark - Preferences	?	x
	WEP and WPA Decryption Keys ? X		
	Key type         Key           wpa-psk         ddb0b09a7d6980515825950b5929d02/236799f3e8a87f163c8ca41a066d8b3b           wpa-psk         7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e		
<.	+ - Pa A V B OK Cancel Help OK Cancel	Help	

해독된 802.11 패킷의 예

File Edit	View Go Capture Analyze Statistics T	Telephony Wireless Tools Help			
	۵ 🎚 🖻 🗙 🖸 ۹ 🗢 🕾 🗑 🕸	💶 🖻 Q. Q. Q. II			
wlan.addr	==04:f1:28:6a:69:11				🔀 🔜 💌 Expression 🕂
No	Time	Source	Destination	Protocol	enath 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 (84:f1:28:6a:69:11) (84)	802.11	45 Request-to-send, Elags=
	397879 2018-11-16 00:17:08.097877	Cisco b4:3d:e4 (00:a3:8e:b4:3d:e4) (T_	HmdGloba 6a:69:11 (84:f1:28:6a:69:11) (84)	802.11	45 Request-to-send, Flags=C
i.	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] 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 (04:11:28:6a:69:11) (RA)	802.11	5/ 802.11 Block Ack, Flags=
	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 3	97886: 154 bytes on wire (1232 bits),	154 bytes captured (1232 bits)			
Radiota	p Header v0, Length 48				
▶ 802.11	radio information				
▷ IEEE 80	2.11 QoS Data, Flags: .pTC				
Logical	-Link Control				
Interne	t Protocol Version 4, Src: 172.16.255	.13, Dst: 40.127.66.24			
Transmi	ssion Control Protocol, Src Port: 456	58, Dst Port: 80, Seq: 128, Ack: 4001196	i, Len: 0		
0000 000	00 30 00 6b 08 1c 00 6d f9 30 31 00 0	00 00 00 ··O·k··· m·01····			
0010 14 0	00 9e 09 80 04 d9 a4 00 00 00 00 80 0	84 81 88			
0020 9e 0		60 00 00 ·····e			
0030 08 0	ac 29 28 89 dd 50 06 00 08 c8 84 00	20 01 00 ··)(··P·····			
0050 00	00 af f4 c2 2f 90 d1 14 52 a5 8b 2e 1	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 (	88 7a 36 57 cd e2 43 89 86 f5 92 24 1	17 d0 db \·z6₩··C ····\$···			
0080 42	a2 2e 62 35 c7 36 9b 54 d0 00 91 78	7d 44 87 Bb5-6- Tx}D-			
0090 23 (	bc /D eb fd db e7 06 39 11	#1( 8-			

PMK가 포함되지 않은 두 번째 결과를 PMK가 포함된 첫 번째 결과와 비교할 경우 패킷 397886은 802.11 QoS 데이터로 해독됩니다.

#### 암호화된 802.11 패킷의 예

Test         Gozze         Destation         Petical         Length Info           337681 2081-11-6 00:17:08.09833         Mmarz_28:09:04         Heddloba_5a:69:11         802.11         138 005 Data, Sh-1438, FH-0, Flags-pF.C           397682 2081-11-6 00:17:08.09844         Mmarz_28:09:04         Heddloba_5a:69:11         802.11         134 025 Data, Sh-1438, FH-0, Flags-pF.C           397682 2081-11-6 00:17:08.09899         Mmarz_28:09:04         Heddloba_5a:69:11         802.11         134 025 Data, Sh-1438, FH-0, Flags-pF.C           397682 2081-11-6 00:17:08.09899         Mmarz_28:09:04         Heddloba_5a:69:11         802.11         146 026 Data, Sh-1637, FH-0, Flags-pF.C           397687 2081-11-6 00:17:08.09895         Mmarz_28:09:04         Heddloba_5a:69:11         802.11         154 025 Data, Sh-128, FH-0, Flags-pF.C           397687 2081-11-6 00:17:08.09895         Heddloba_5a:69:11         Wmarz_28:09:04         802.11         57 082.11 Block Ack, Flags-pF.C           397687 2081-11-6 00:17:08.09895         Heddloba_5a:69:11         Wmarz_28:09:04         Heddloba_5a:69:11         802.11         57 082.11 Block Ack, Flags-pF.C           397687 2081-11-6 00:17:08.09805         Wmarz_28:09:04         Heddloba_5a:69:11         802.11         57 082.11 Block Ack, Flags-pC           397687 2081-11-6 00:17:08.09805         Wmarz_28:09:04         Heddloba_6a:69:11	vlan.addr	==04:f1:28:6a:69:11				Expres
97821 2012-11-16 00:17:08.09834       Wmare 28:09:04       HedGloba_Ga:69:11       802.11       1438 050 Data, SH:435, HHe, Flags-, p, F.C.         978783 2018-11-16 00:17:08.09844       HedGloba_Ga:69:11       002.11       1340 Data (So Data, SH:435, HHe, Flags-, p, F.C.         978783 2018-11-16 00:17:08.09894       HedGloba_Ga:69:11       Vmare 28:09:04       802.11       57 002.11 Block Ack, Flags-, p, F.C.         978785 2018-11-16 00:17:08.09999       HedGloba_Ga:69:11       Vmare 28:09:04       802.11       57 002.11 Block Ack, Flags-, p, TC         978785 2018-11-16 00:17:08.09991       HedGloba_Ga:69:11       Vmare 28:09:04       802.11       134 05 Data, SH:435, HHe, Flags-, p, TC         978785 2018-11-16 00:17:08.09901       HedGloba_Ga:69:11       Vmare 28:09:04       802.11       57 002.11 Block Ack, Flags-, p, TC         978785 2018-11-16 00:17:08.09127       HedGloba_Ga:69:11       Vmare 28:09:04       802.11       57 002.11 Block Ack, Flags-, p, TC         978785 2018-11-16 00:17:08.0122       Clics_bH:3d:c4 (00:13:08:04:13:04:04)       TmedGloba_Ga:69:11       802.11       57 002.11 Block Ack, Flags-, p, F.C.         978785 2018-11-16 00:17:08.0123       Clics_bH:3d:c4 (00:13:08:04:13:04:04)       HedGloba_Ga:69:11       802.11       57 002.11 Block Ack, Flags-, p, F.C.         978785 2018-11-16 00:17:08.0123       Clics_bH:3d:c4 (00:13:08:04:13:04:04)       HedGloba_Ga:69:11		Time	Source	Destination	Protocol	Length Info
97882 2018-11:6 00:17:08.09444       Wmar_28:09:04       HedGlob_6:0:0911       802.11       154 005 Data; SH=1435; FH=0; Flags,F.C         97883 2018-11:6 00:17:08.09494       Wmar_28:09:04       HedGlob_6:0:0911       802.11       155 005 Data; SH=1435; FH=0; Flags,F.C         97884 2018-11:6 00:17:08.09499       Wmar_28:09:04       HedGlob_6:0:011       802.11       156 005 Data; SH=1435; FH=0; Flags,F.C         97885 2018-11:16 00:17:08.09409       Wmar_28:09:04       HedGlob_6:0:10       Wmar_28:09:04       802.11         97885 2018-11:16 00:17:08.09409       Mmar_28:09:04       HedGlob_6:0:10       Wmar_28:09:04       802.11         97885 2018-11:16 00:17:08.09405       Gicc_Jstire4 (00:13):Erbt3:104 (01:128:6:109:11) (04:1]       154 005 Data; SH=143; FH=0; Flags,C         97888 2018-11:16 00:17:08.09405       HedGlob_6:0:10       Wmar_28:09:04       802.11       155 005 Data; SH=143; FH=0; Flags,C         97889 2018-11:16 00:17:08.09405       HedGlob_6:0:10       Wmar_28:09:04       802.11       155 005 Data; SH=143; FH=0; Flags,C         97898 2018-11:16 00:17:08.09405       Wmar_28:09:04       HedGlob_6:0:05:01       Wmar_28:09:01       802.11       155 005 Data; SH=143; FH=0; Flags,C         19789 2018-11:16 00:17:08.09405       Wmar_28:09:04       HedGlob_6:0:05:01       HedGlob_6:0:05:01       802.11       150 005 Data; SH=143; FH=0; Flags,		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
997833 2018-11-16 00:17:08.09999       HudGloba_6s:09:11       Cisco_b4:16:44 (00:03:36:16:14:14)       802.11       57 802.11       Block Ack; Flags         99783 2018-11-16 00:17:08.09999       HudGloba_6s:09:11       Wmarz_28:09:1d       802.11       15 606 50rts, 50:4435; ref. (40; Flags,rc         99783 2018-11-16 00:17:08.09099       HudGloba_6s:09:11       Wmarz_28:09:1d       802.11       15 605 50rts, 50:4435; ref. (40; Flags,rc         99783 2018-11-16 00:17:08.09095       HudGloba_6s:09:11       Wmarz_28:09:1d       802.11       15 605 50rts, 50:403; ref. (10; Flags,rc         99783 2018-11-16 00:17:08.09056       Cisco_b4:13:de:4(00:13:80:45:4):40:41; L28:6a:69:11)       802.11       15 605 50rts, 50:403; ref. (10; Flags,rc         99789 2018-11-16 00:17:08.09055       Cisco_b4:13:de:4(00:13:80:14:24:14:4)       (T. HudGloba_6s:69:11)       802.11       57 802.11 850; Ref. (10; Flags,rc         99789 2018-11-16 00:17:08.108055       Wmarz_28:09:dd       HudGloba_6s:69:11       Wmarz_28:09:dd       802.11       57 802.11 850; Ref. (10; Flags,rc         99789 2018-11-16 00:17:08.09055       Cisco_b4:13:de:4(00:13:80:16:06:11)       HudGloba_6s:69:11       802.11       57 802.11 850; Ref. (10; Flags,rc         99789 2018-11-16 00:17:08.09055       Wmarz_28:19:0d       HudGloba_6s:09:11       802.11       57 805 20:14; Flags,rc       15 802.11 10:10:10:10:10:10:10:10:10:10:10:10:10:1		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
397864 2018-11-16 00:17:08.09999 Vmsrc 21:89:dd       Hediobs 2:09:11       00:11       00:11       00:11       00:11       00:11       00:11       00:11       10:12       00:11       10:12       00:11       10:12       10:12       00:11       10:12       10:12       00:11       10:12       10:12       00:11       10:12       10:12       00:11       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12       10:12		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
397886 2016-11-16 00:17:08.09909       Heddloba_sr:09:11       Vmarc 28:09:1d       392.11       154 005 Data, 5N=101, FH+0; Flag=*,p,TC         397886 2018-11-16 00:17:08.09906       Heddloba_sr:09:11       Heddloba_sr:09:11       Wmarc 28:09:1d       802.11       154 005 Data, 5N=102, FH+0; Flag=*,p,TC         397886 2018-11-16 00:17:08.099065       Heddloba_sr:09:11       Wmarc 28:09:1d       802.11       154 005 Data, 5N=102, FH+0; Flag=*,p,TC         397880 2018-11-16 00:17:08.109552       Vmarc 28:09:1d       Wmarc 28:09:1d       802.11       57 005 Data, 5N=102, FH+0; Flag=*,p,TC         397892 2018-11-16 00:17:08.109552       Vmarc 28:09:1d       Heddloba_sr:09:11       (41f1:128:6a:69:11) (A1f1)       802.11       57 802.11 Block Ack, Flags*.p,FC         397892 2018-11-16 00:17:08.108555       Vmarc 28:09:1d       Heddloba_sr:09:11       (41f1:128:6a:69:11) (A1f1)       802.11       57 802.11 Block Ack, Flags*.p,FC         397892 2018-11-16 00:17:08.108555       Vmarc 28:09:1d       Heddloba_sr:09:11       (41f1:128:6a:69:11) (A1f1)       802.11       55 805 Data, 5N=1437, FH+0; Flags*.p,FC         397892 2018-11-16 00:17:08.108555       Vmarc 28:09:1d       Heddloba_sr:09:11       (41f1:128:6a:69:11) (A1f1)       802.11       55 805 Data, 5N=137, FH+0; Flags*.p,FC         397892 2018-11-16 00:17:08.108555       Vmarc 28:09:1d       Heddloba_sr:09:11       Heddloba_sr:09:11 <t< td=""><td></td><td>397884 2018-11-16 00:17:08.098999</td><td>Vmware 28:89:dd</td><td>HmdGloba 6a:69:11</td><td>802.11</td><td>162 QoS Data, SN-1436, FN-0, FlagspF.C</td></t<>		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
97887 2012-11-16 00:17:08.090121       Cisco_b47:3dre4 (00:a3:8:10+13dre4) (TL = HedGloba_a5:n0:11 (44:f1:28:6a:60:11) (AA)       802.11       >> 000:11 010ck acks, flags=C         97889 2013-11-16 00:17:08.099655       Cisco_b47:3dre4 (00:a3:8:10+13dre4) (TL = HedGloba_a5:60:11) (AA)       802.11       55 005 Dats, 51:102, FH:0F, Flags=.p,TC         97899 2013-11-16 00:17:08.101762       HedGloba_a5:60:11       (HedGloba_a5:60:11) (AA: f1:28:6a:60:11) (AA)       802.11       55 802.11 Block Ack, flags=C         97899 2013-11-16 00:17:08.10182       HedGloba_a5:60:11       (HedGloba_a5:60:11) (AA: f1:28:6a:60:11) (AA)       802.11       55 802.11 Block Ack, flags=C         97989 2013-11-16 00:17:08.10182       HedGloba_a5:60:11       802.11       55 802.11 Block Ack, flags=,C         97989 2013-11-16 00:17:08.100182       HedGloba_a5:60:11       802.11       55 802.11 Block Ack, flags=,C         97989 2013-11-16 00:17:08.100182       HedGloba_a5:60:11       802.11       55 802.11 Block Ack, flags=,F.C         97899 2013-11-16 00:17:08.100182       HedGloba_a5:60:11       802.11       156 QO Dats, 51Hags=.p,F.C         97899 2013-11-16 00:17:08.100182       HedGloba_a5:60:11       802.11       156 QO Dats, 51Hags=.p,F.C         97899 2013-11-16 00:17:08.100182       HedGloba_a5:60:11       802.11       156 QO Dats, 51Hags=.p,F.C         97899 2013-115 Hotts       HedGloba_a5:60:11		397886 2018-11-16 00:17:08.099099	HmdGloba 6a:69:11	Vmware 28:89:dd	802.11	154 OoS Data, SN=101, FN=0, Flags=.pTC
97888 2018-11-16 00:17:08.099666       HedGlobs_61:69:11       Wmare_28:89:1d       802.11       154 QOS Data, SH=30; FH=0; Flags+C         97889 2018-11-6 00:17:08.099666       HedGlobs_61:69:11       Wmare_28:89:1d       802.11       154 QOS Data, SH=30; FH=0; Flags+C         97899 2018-11-6 00:17:08.0912       HedGlobs_61:69:11       Wmare_28:89:1d       802.11       154 QOS Data, SH=30; FH=0; Flags+C         97899 2018-11-6 00:17:08.0912       Clisco_b1:31:e4 (00:13:02:104:4) (TL HedGlobs_61:69:11 (00:11:28:63:69:11) (RA)       802.11       55 QOS Data, SH=437; FH=0; Flags+C         97898 2018-11-16 00:17:08.09255       Wmare_28:89:dd       HmdGlobs_61:69:11       802.11       55 QOS Data, SH=437; FH=0; Flags+C         97898 2018-11-16 00:17:08.09255       Wmare_28:89:dd       HmdGlobs_61:69:11       802.11       55 QOS Data, SH=437; FH=0; Flags+C         97898 2018-11-16 00:17:08.09255       Wmare_28:89:dd       HmdGlobs_61:69:11       802.11       154 QOS Data, SH=437; FH=0; Flags+C         97898 2018-11-16 00:17:08.09256       Wmare_28:89:dd       HmdGlobs_61:69:11       802.11       154 QOS Data, SH=437; FH=0; Flags+C         97898 2018-11-16 00:17:08.09256       Wmare_28:89:dd       HmdGlobs_61:69:11       802.11       154 QOS Data, SH=437; FH=0; Flags+C         9211 radio Information       E       E       E       E       E       <		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	57 602.11 Block Ack, Flags=
97859 2018-11-16 00:17:08.09555 Clisco_45_3d:e4 (00:a3:de:Ubi3d:e4) (T.= HudGloba_Ga:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 97892 2018-11-16 00:17:08.108122 Clisco_b4:3d:e4 (00:a3:Be:Ubi3d:e4) (T.= HudGloba_Ga:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 97892 2018-11-16 00:17:08.108122 Clisco_b4:3d:e4 (00:a3:Be:Ubi3d:e4) (T.= HudGloba_Ga:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 97892 2018-11-16 00:17:08.10852 Mmare 22:09:dd HudGloba_Ga:69:11 (04:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 97892 2018-11-16 00:17:08.108555 Mmare 22:09:dd HudGloba_Ga:69:11 (84:f1:28:6a:69:11) (RA) 802.11 57 802.11 Block Ack, Flags=C 97892 2018-11-16 00:17:08.10855 Mmare 22:09:dd HudGloba_Ga:69:11 802.11 59 805 Data, Sh=438, FH=0, Flags=.pF.C HudGloba_Ga:69:11 802.11 602.11 59 805 Data, Sh=438, FH=0, Flags=.pF.C 14 adotap Header V0, Length 43 02.11 radio information 826 802.11 GoS Data, Flags: .pTC ata (68 bytes) 96 90 80 90 60 60 80 60 60 80 60 60 00 00 00 00 00 00 00 00 00 00 00		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
997899 2018-11-16 001:77:08.101762       HedGloba_6a:69:11       Vmaxre_23:08:dd       802.11       479 QoS Data, SH=03, Flags=.pTC         397891 2018-11-16 001:77:08.105958       Vmaxre_23:08:dd       HedGloba_6a:69:11 (04:11:28:6a:69:11) (04:11:28:		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
397891 2018-11-16 00:17:08.101312       Cisco_b673d:e4 (00:a3:8e:b4:3d:e4) (THodGloba_6a:69:11) (RA)       802.11       57 802.11 Block Ack, Flags=C         397892 2018-11-16 00:17:08.105058       Wmware_28:89:dd       HmdGloba_6a:69:11       802.11       55 005 Data, SN=1435, FN=0, FLG         1000000000000000000000000000000000000		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
397892 2013-11-16 00:17:08.109958       Vmware 28:89:dd       HedGloba_5a:69:11       602.11       595 QoS Data, SN=1437, FN=0, Flags=, pF.C         397894 2013-11-16 00:17:08.109056       Vmware 28:89:dd       HedGloba_5a:69:11       602.11       154 QoS Data, SN=1437, FN=0, Flags=, pF.C         rame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)       Estensor       123       123       124		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
397294 2018-11-16 00:17:08.106055 Vmwarz 28:89:dd       HmdGloba_6a:69:11       802.11       154 QoS Data, SN=1438, FN=0, Flags=.pF.C         rame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)       HmdGloba_6a:69:11       802.11       154 QoS Data, SN=1438, FN=0, Flags=.pF.C         rame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)       HmdGloba_6a:69:11       802.11       154 QoS Data, SN=1438, FN=0, Flags=.pF.C         rame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)       If add of the second of the seco		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
rame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)         adiotap Header v0, Length 48         02.11 radio information         EEE 802.11 QoS Data, Flags: .pTC         ata (68 bytes)         0         0       00 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 00 00 .0 .0 .0 .0 .0 .0 .0 .0 .0		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
rame 397886: 154 bytes on wire (1232 bits), 154 bytes captured (1232 bits)         adiotap Header V0, Length 48         0.11 radio information         EEE 802.11 QoS Data, Flags: .pTC         ata (68 bytes)         0         0       00 00 30 00 6b 08 1c 00 6d f9 30 31 00 00 00 0       -0.kc. m.01         14 00 9c 99 80 04 69 44 00 00 00 00 0       -0.kc. m.01         9c 90 0b 22 1f 00 06 00 65 00 81 06 40 00 00 0       -0.kc. m.01         0       00 00 30 00 6b 08 1c 00 40 40 00 00 0       -0.kc. m.01         0 84 13 06 00 00 28 06 40 10 0						
0       00       00       6b       10       00						
0       00       00       6b       81       100       6d       19       101       00 <t< th=""><th></th><th></th><th></th><th></th><th></th><th></th></t<>						
0       00						
00       00 <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<>						
00       00 <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td></td<>						
0       00						
1 4 40 9e 09 30 09 4 07 34 00 00 00 70 50 94 01 00         9 e0 9 0b 22 1f 60 06 00 55 00 00 00 40 0 10 00 40 0 10 00         0 8 84 13 00 00 00 38 0e 14 32 as 14 12 8 as 69 11         0 00 00 29 28 89 d3 50 60 00 c8 84 00 20 01 00         0 00 00 27 44 c2 2 f 90 d1 14 52 as 58 12 57 27 3         0 48 54 as 55 0a 12 92 da fc as 1f c2 c8 34 39 ca         5 c0 87 33 65 75 cd 2 43 89 86 f5 92 24 17 0d db         0 42 az 2 c6 2 35 c7 36 9b 54 d0 09 91 78 7d 44 87         8 42 az 2 c6 2 35 c7 36 9b 54 d0 09 91 78 7d 44 87	0 00 0	20 30 00 6b 08 1c 00 6d f9 30 31 00 0	00 00 00 ···0·k··· m·01····			
9e       9e <td< td=""><td>14 0</td><td>10 9e 09 80 04 d9 a4 00 00 00 00 80 0</td><td>84 81 88</td><td></td><td></td><td></td></td<>	14 0	10 9e 09 80 04 d9 a4 00 00 00 00 80 0	84 81 88			
00       00       02       28       89       dd       50       00 <td< td=""><td>98 6</td><td>19 00 22 17 00 00 00 55 00 00 00 04 0</td><td>62 69 11 .49</td><td></td><td></td><td></td></td<>	98 6	19 00 22 17 00 00 00 55 00 00 00 04 0	62 69 11 .49			
00       00       00       00       14       52       a5       8b       2e       57       27       3a	0 00 4	ac 29 28 89 dd 58 86 88 88 68 84 88	20 01 00 ···)(··P			
0 d8 54 a5 55 6a 12 92 da fc a9 1f c2 c8 34 39 ca ⊤U		a0 af f4 c2 2f 90 d1 14 52 a5 8b 2e	57 27 3a			
0 5c 08 7a 36 57 cd e2 43 89 86 f5 92 24 17 d0 db \ 26W C ··· \$··· 0 42 a2 2e 62 35 c7 36 9b 54 d0 00 91 78 7d 44 87 B b5 6 T ···x}D·	8 88 6					
0 42 a2 2e 62 35 c7 36 9b 54 d0 00 91 78 7d 44 87 B b5 6 T···x}D	50 00 0	54 a5 55 0a 12 92 da fc a9 1f c2 c8 :	34 39 ca T.U			
	50 00 0 60 d8 5 70 5c 0	54 a5 55 0a 12 92 da fc a9 1f c2 c8 88 7a 36 57 cd e2 43 89 86 f5 92 24 :	34 39 ca ·T·U·····49· 17 d0 db ··c6W··C····\$···			

주의:암호 해독 시 Wireshark에 문제가 발생할 수 있습니다. 이 경우 올바른 PMK가 제공되더 라도(또는 PSK가 사용된 경우 SSID와 PSK가 모두 제공됨) Wireshark는 OTA 캡처를 해독하 지 않습니다.해결 방법은 상위 계층 정보를 얻고 802.11 패킷이 더 이상 QoS 데이터로 표시되 지 않을 때까지 Wireshark를 끄고 몇 번 켜거나 Wireshark가 설치된 다른 PC/Mac을 사용하는 것입니다.

팁: 관련 정보의 첫 번째 게시물에 pmkXtract라는 C++ 코드가 첨부됩니다.컴파일된 시도가 성

공적으로 수행되고 실행 파일을 가져오기는 했지만 알려진 이유로 실행 프로그램에서 해독을 제대로 수행하지 않는 것 같습니다.또한 PMK를 추출하려는 Python 스크립트가 첫 번째 게시 물의 의견 영역에 게시되어 독자가 관심이 있을 경우 더 자세히 살펴볼 수 있습니다.

## 관련 정보

- EAP의 취약한 링크 조정 pmkXtract를 사용하여 RADIUS에서 WiFi PMK 재생
- <u>RADIUS MS-MPPE-Recv-Key를 디코딩하는 방법</u>
- <u>기술 지원 및 문서 Cisco Systems</u>