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

목차

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 권장되지는 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(인증자에서 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.

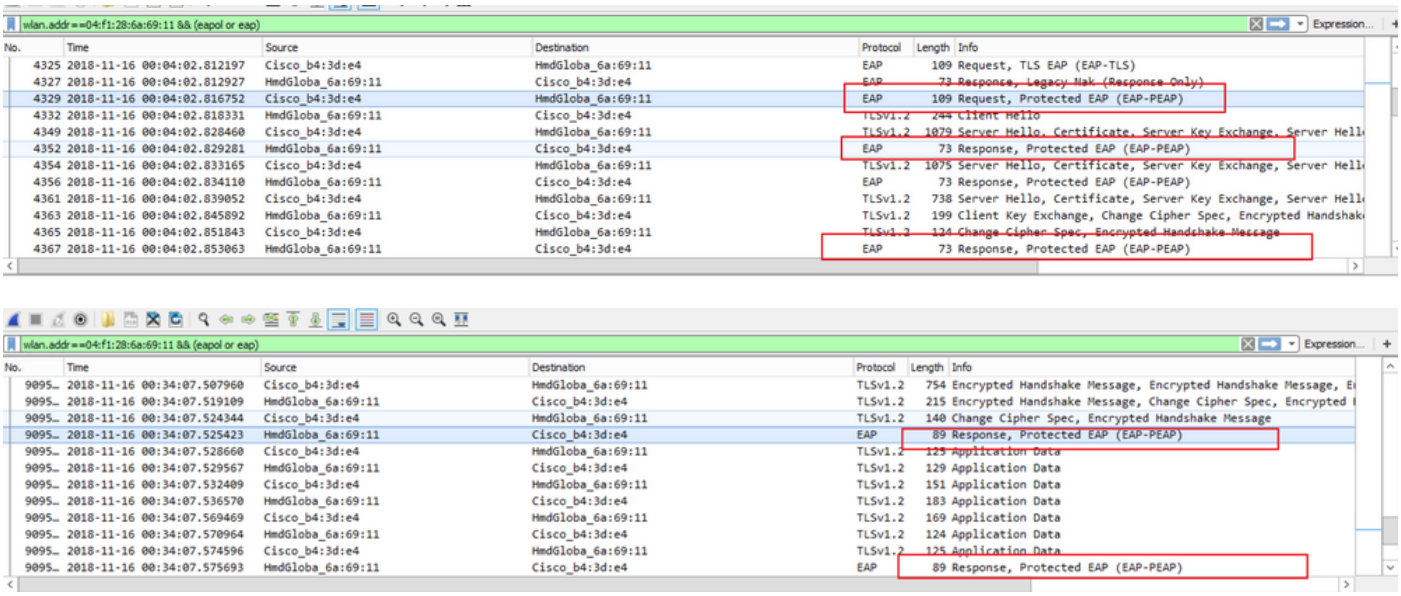
- Radius 서버(FreeRADIUS 또는 ISE)
- Over-the-Air 캡처 장치
- Apple macOS/OS X 또는 Linux 디바이스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 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.



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 설정되고 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>

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 = 0x52656175746853657373696f6e3a30613432346632613030303030356537356265653039373 2

Class =
0x434143533a30613432346632613030303030356537356265653039373 23a4953452d322d332f333238323731323338
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 = 0x52656175746853657373696f6e3a30613432346632613030303030356537356265653039373 2

Class =
0x434143533a30613432346632613030303030356537356265653039373 23a4953452d322d332f333238323731323338
2f33303434

EAP-Message = 0x03910004

Message-Authenticator = 0x81c572651679e15e54a900f3360c0aa9

MS-MPPE-Send-Key = 0xeae42cf7c6cd26371eee29856c51824fbb5bbb298874125928470114d009b5fb

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

Authenticator-Field = 0xa523dd9ec2ce93d19fe4fc2e21537a5d
```

참고:RADIUS 패킷 캡처의 가상 LAN(VLAN) 태그를 제거하십시오. 그렇지 않으면 **radsniff**에서 입력 pcap 파일을 인식하지 못합니다.예를 들어, VLAN 태그를 제거하려면 editcap을 사용할 수 있습니다.

팁:일반적으로 RADIUS pcap 파일에 **대한** radsniff 명령의 런타임을 초 단위로 계산할 수 있습니다.그러나 **radsniff**가 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

Logging all events
```

```
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)

ISE Tcpdump(B)

병합됨(A+B)

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

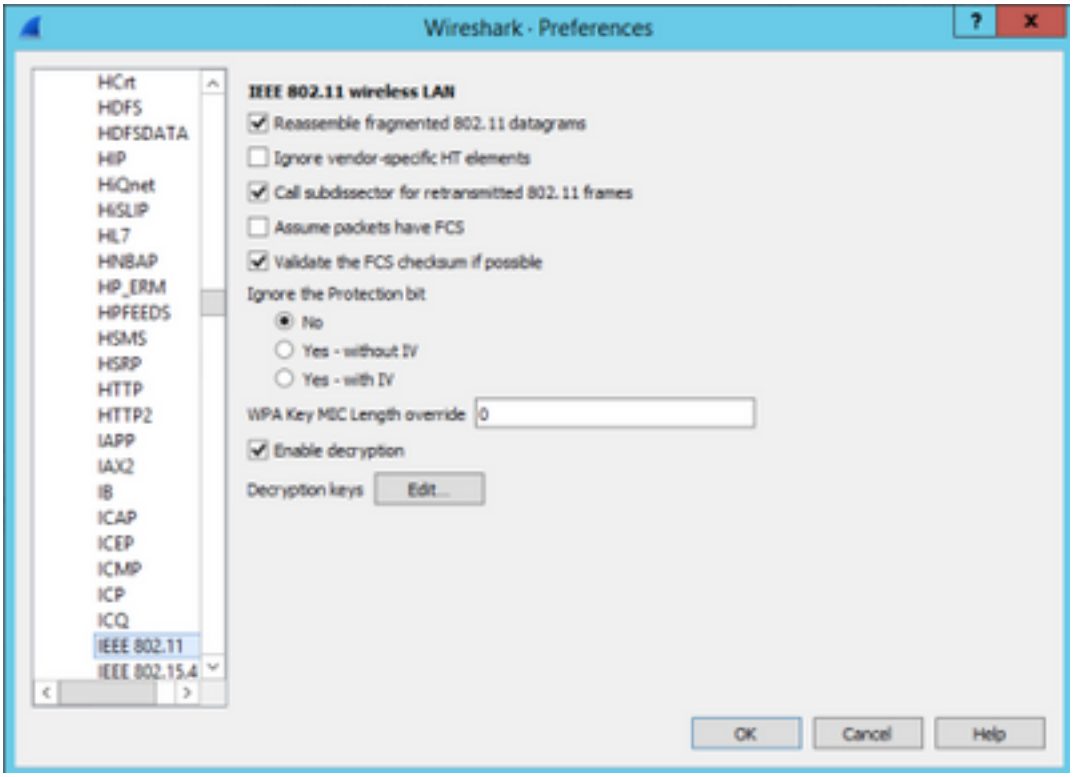
```
PMK:
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d7984816a3793c5a4dfb1cfb0e

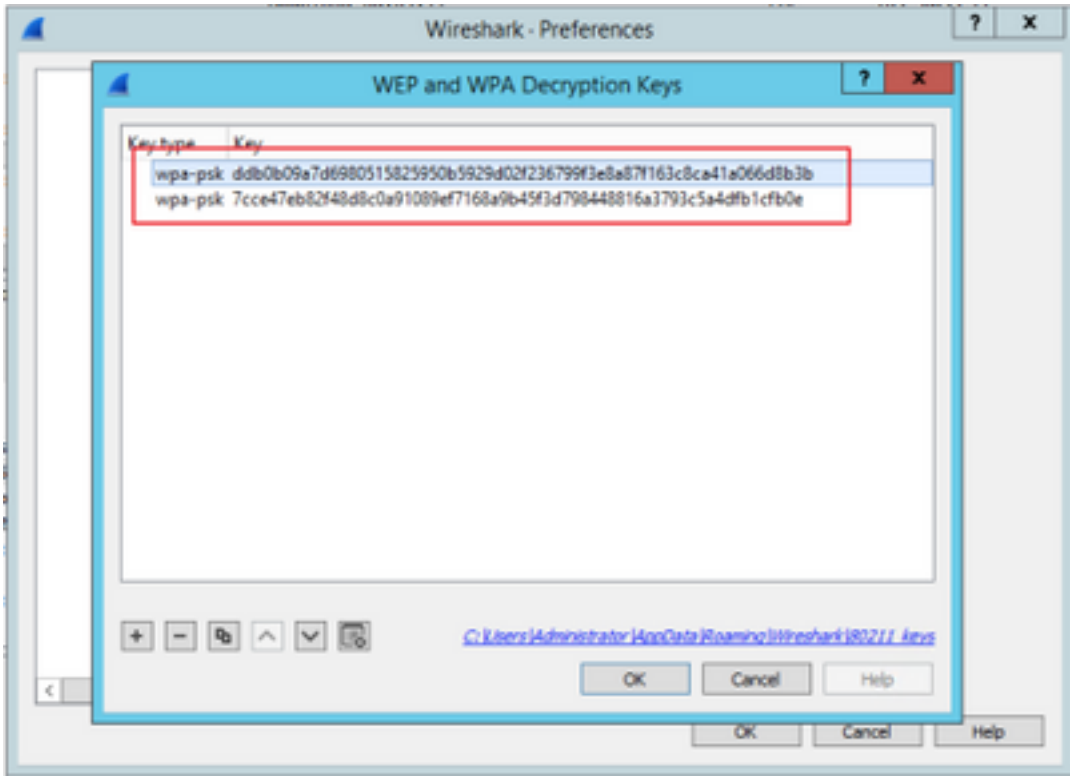
```
PMK:
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e
```

3단계. OTA 스니퍼를 해독합니다.

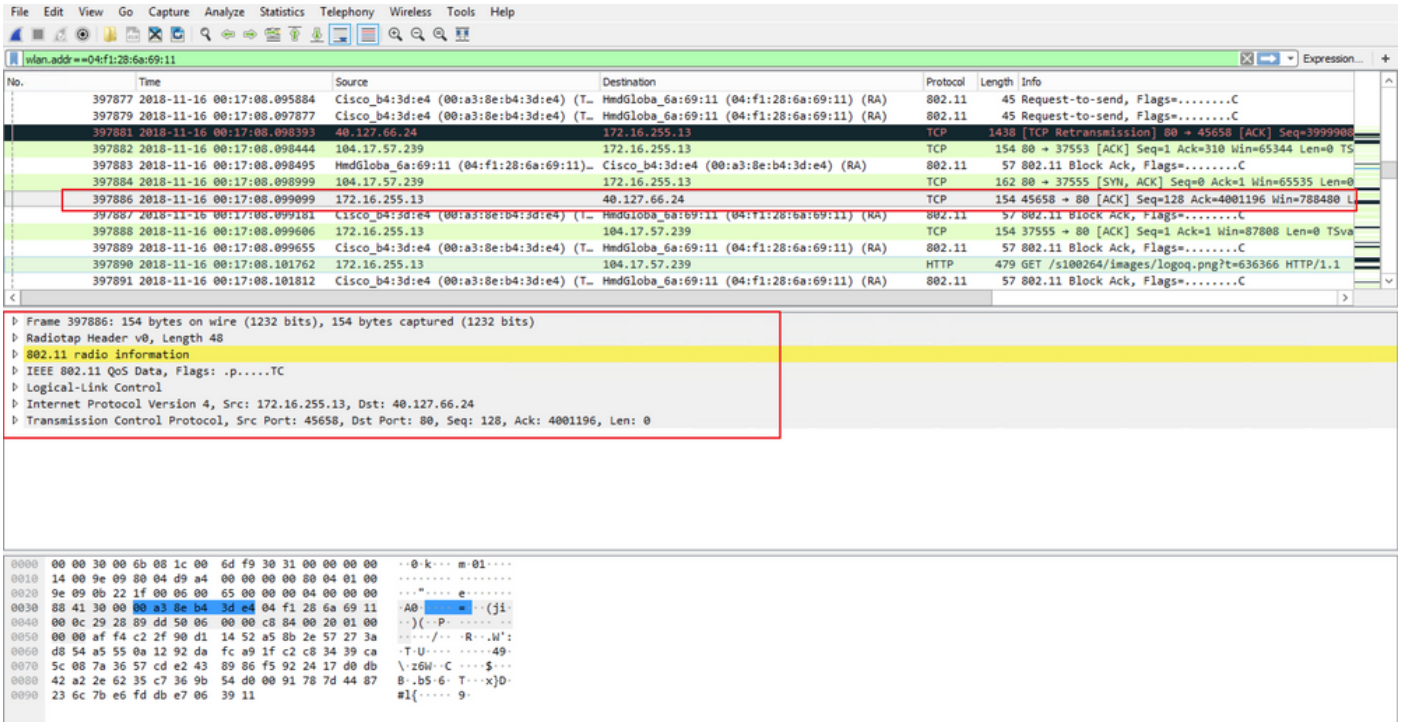
Wireshark **> Preferences > Protocols > IEEE 802.11로** 이동한 다음 **Enable Decryption(암호 해독 활성화)**을 선택하고 이미지에 표시된 것처럼 Decryption Keys(암호 해독 키) 옆의 Edit(수정) 버튼을 클릭합니다.



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

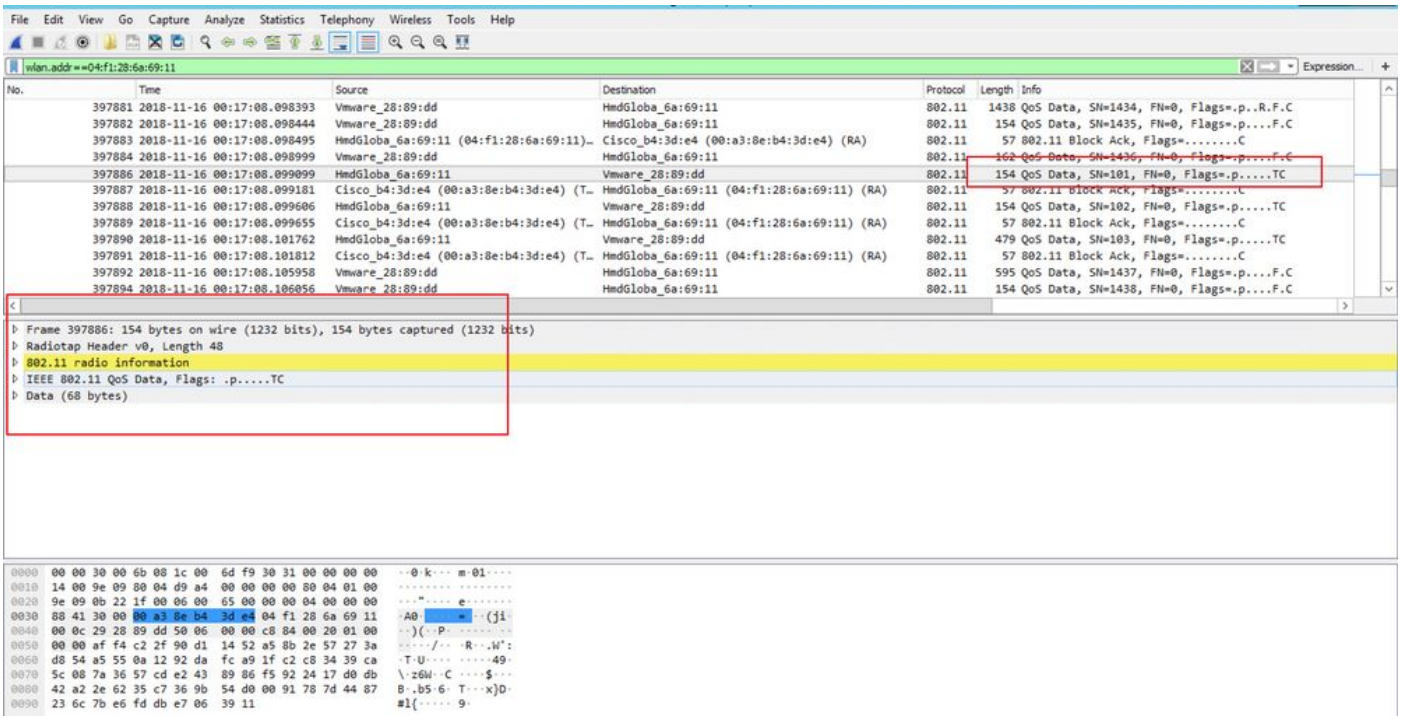


해독된 802.11 패킷의 예



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



주의:암호 해독 시 Wireshark에 문제가 발생할 수 있습니다. 이 경우 올바른 PMK가 제공되더라도(또는 PSK가 사용된 경우 SSID와 PSK가 모두 제공됨) Wireshark는 OTA 캡처를 해독하지 않습니다.해결 방법은 상위 계층 정보를 얻고 802.11 패킷이 더 이상 QoS 데이터로 표시되지 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 게시물의 의견 영역에 게시되어 독자가 관심이 있을 경우 더 자세히 살펴볼 수 있습니다.

관련 정보

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