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

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[步骤](#)
[步骤1.从Access-accept数据包解密PMK。](#)
[步骤2.提取PMK。](#)
[步骤3.解密OTA嗅探器。](#)
[解密的802.11数据包示例](#)
[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：

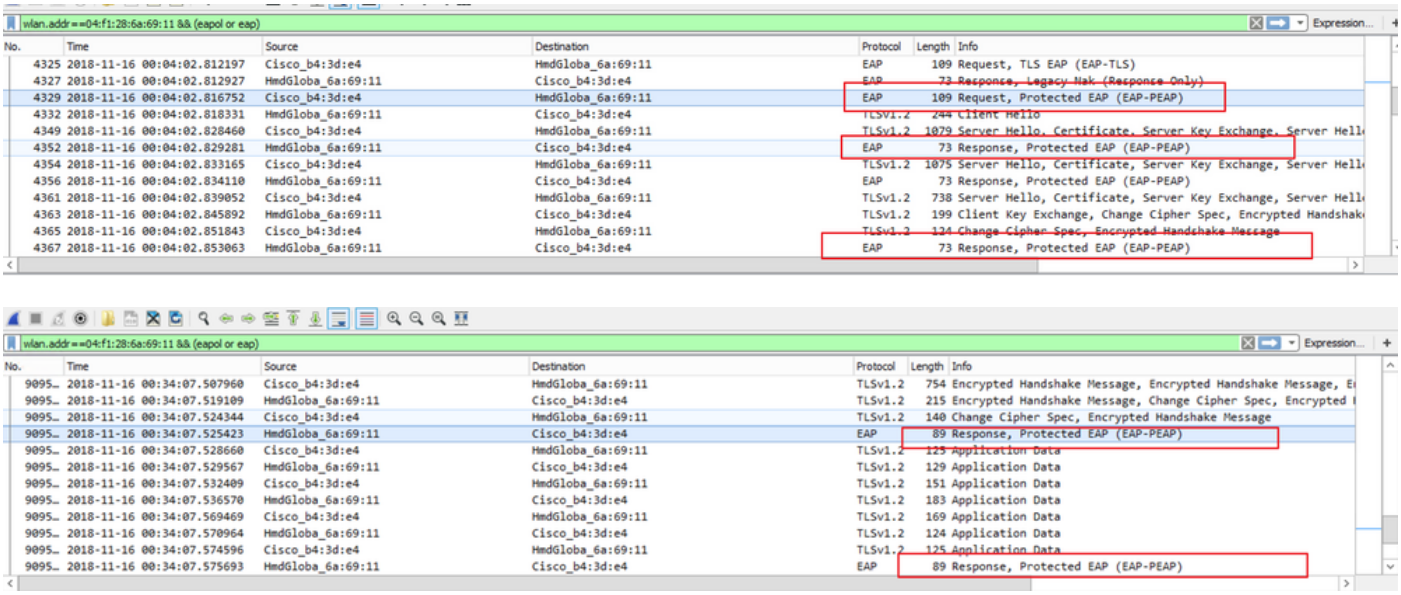
- Radius服务器（FreeRADIUS或ISE）
- 空中捕获设备
- Apple macOS/OS X或Linux设备

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。



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access-accept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 = 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
```

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，可使用editcap。

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 Cisco123 -x

Logging all events

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

在本示例中，通过WLC数据包日志记录功能捕获的无线局域网控制器(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)

ISE Tcpdump(B)

合并(A+B)

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

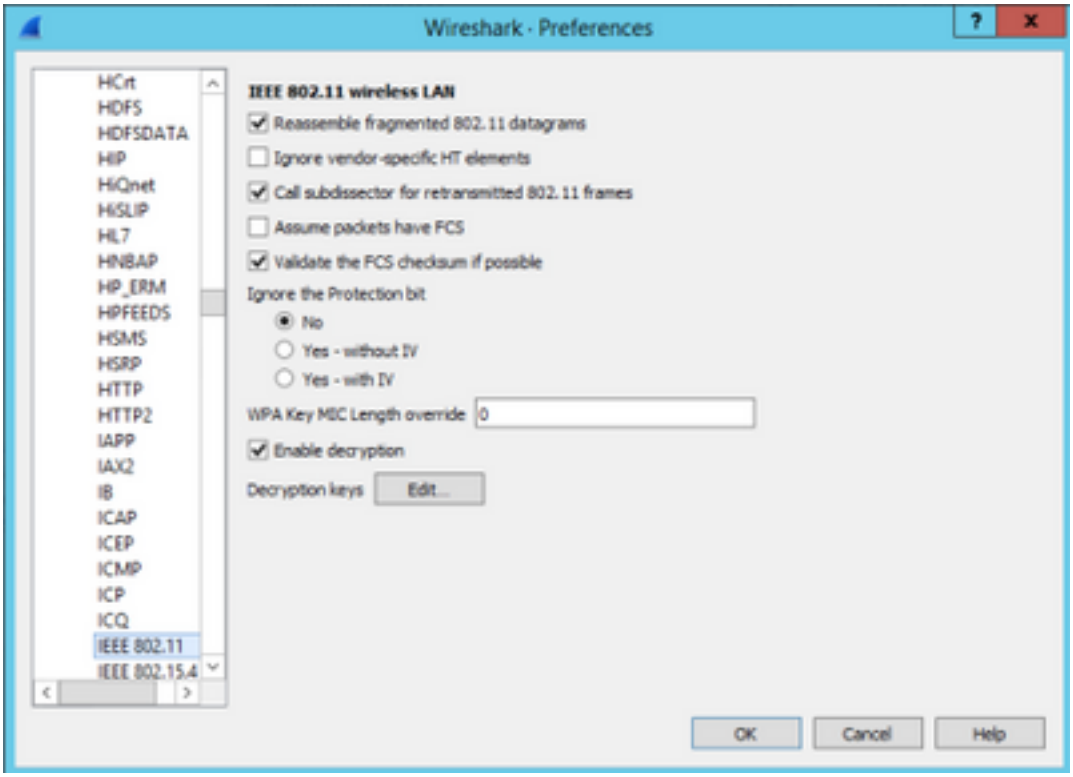
```
PMK:
ddb0b09a7d6980515825950b5929d02f236799f3e8a87f163c8ca41a066d8b3b
```

MS-MPPE-Recv-Key = 0x7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e

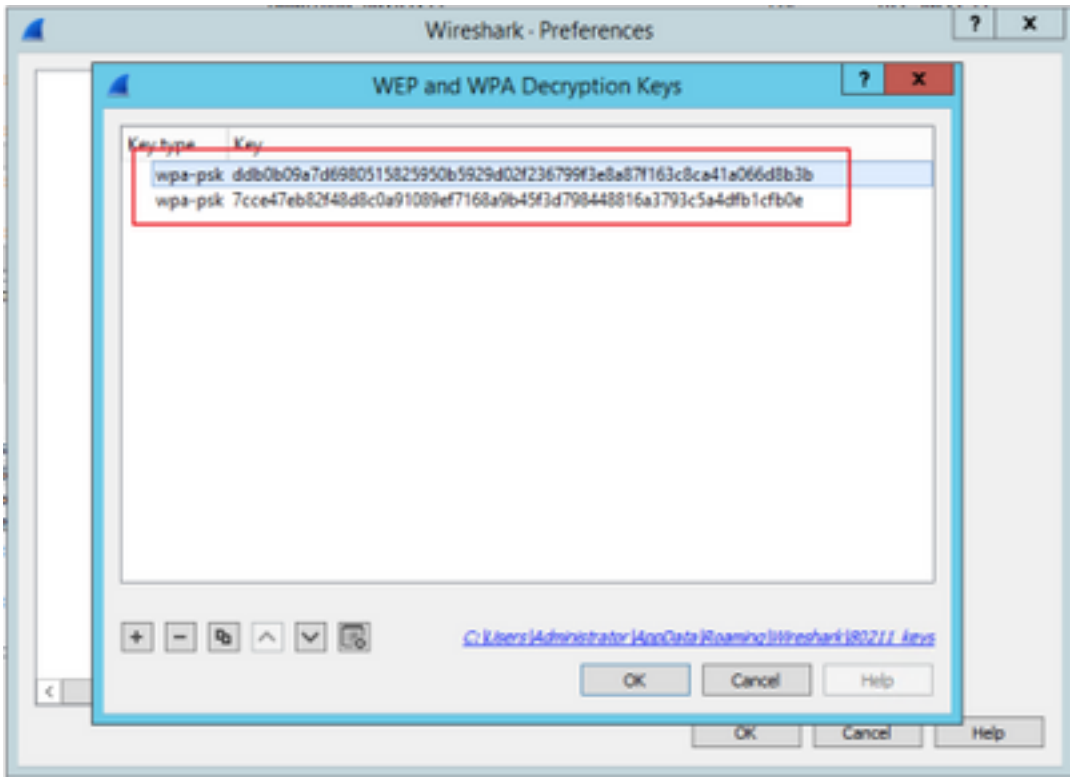
```
PMK:
7cce47eb82f48d8c0a91089ef7168a9b45f3d798448816a3793c5a4dfb1cfb0e
```

步骤3.解密OTA嗅探器。

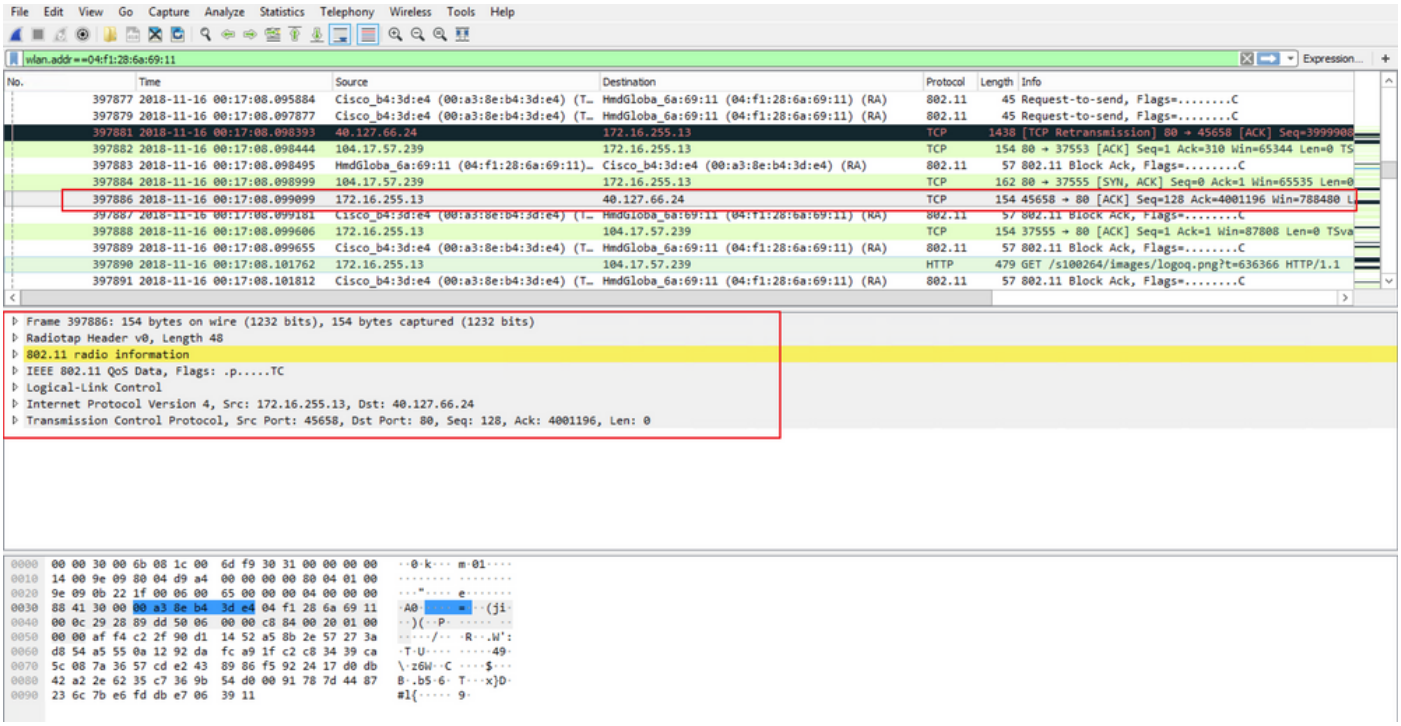
导航至**Wireshark > Preferences > Protocols > IEEE 802.11。然后，选中Enable Decryption**，然后单击**Decryption Keys**旁边的**Edit**按钮，如图所示。



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。

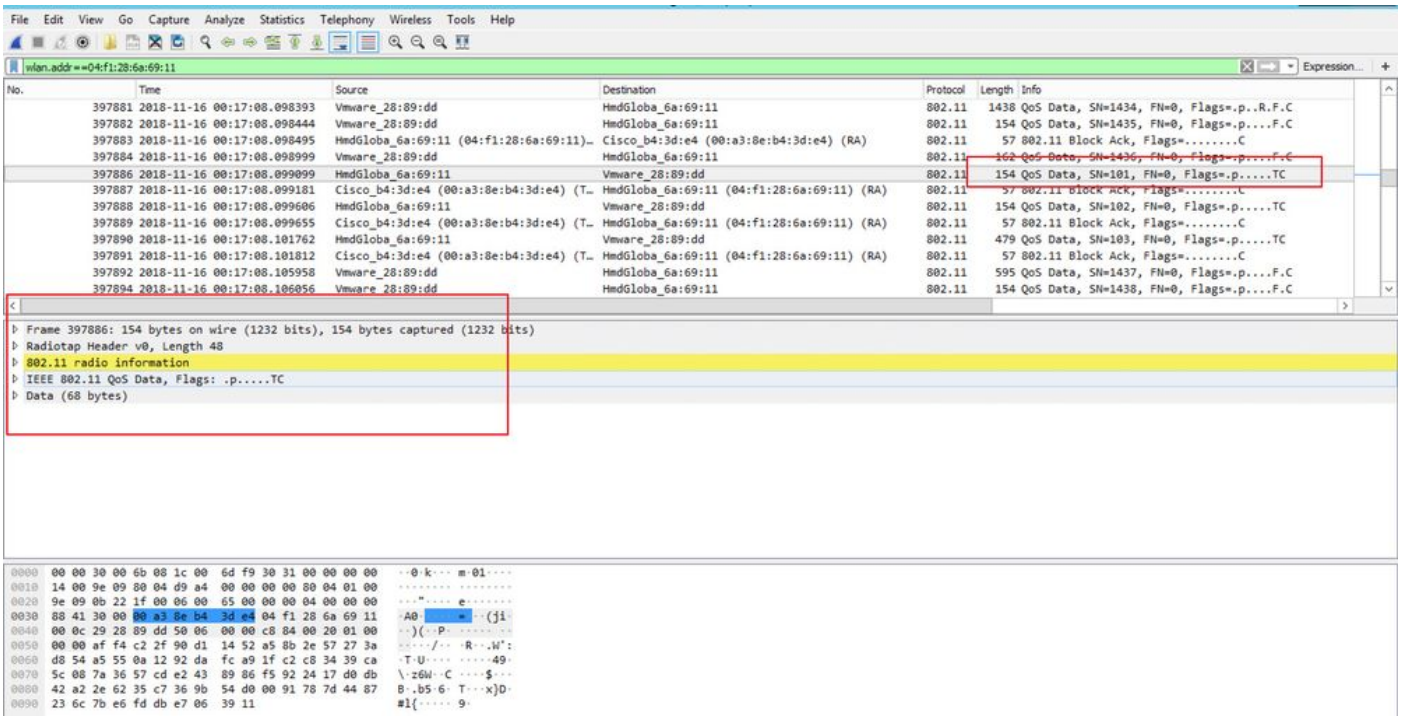


解密的802.11数据包示例



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



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
- 技术支持和文档 - Cisco Systems