**WPA3 lab**

In this lab, we will look at one of the most recent, next generation of Wi-Fi security, WiFi Protected Access 3 (WPA3)-Personal with SAE (Simultaneous Authentication of Equals). WPA3 adds new features to simplify Wi-Fi security, enables more robust authentication, and delivers increased cryptographic strength for highly sensitive data.

Here are some additional background readings:

1. <https://www.wi-fi.org/discover-wi-fi/security>
2. [https:*//*wi-fi.org*/*download.php?file*=/*sites*/*default*/*files*/*private*/*WPA3\_Specification\_v2.0.pdf](https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v2.0.pdf)
3. <https://sarwiki.informatik.hu-berlin.de/WPA3_Dragonfly_Handshake>

In Wireshark labs we can easily capture frames on a wired Ethernet connection. Here, since 802.11 is a wireless link-layer protocol, we’ll be capturing frames “in the air.” Unfortunately, many device drivers for wireless 802.11 NICs don’t provide the hooks to capture/copy received 802.11 frames for use in Wireshark.

If you are using a Linux system you can typically capture WiFi packets however this is not always the case for Windows systems. Thus, in this lab, we’ll provide a trace of captured 802.11 frames with WPA3 protocol for you to analyze and assume in the questions below that you are using this trace.

**1. Getting Started**

Download the packet trace: wpa3-sae.pcapng

This pcap file was taken from a public repository of pcap files for this lab. In this trace file, we’ll see frames captured on channel 3. We will focus on data packets necessary for completing the SAE handshake, namely: four Authentication frames to makeup SAE handshake, followed by Association Request and Response, and finally EAPOL four-way handshake (M1-M4 messages).

The wireless host activities taken in the trace file are:

* We see that the AP is sending out Beacon frames.
* At t=0.353s the client initiates the SAE handshake, first phase, by sending SAE authentication commit.
* At t= 0.455s the client and AP initiate the second phase by sending each other Association request and Response.
* At t=0.464s, the third phase, 4-Way handshake is carried out to facilitate data exchange.

Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the pcap trace file.

**2. Beacon Frames:**

Beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you’ll want to look at the details of the “IEEE 802.11” frame and subfields in the middle Wireshark window.

Table

Description automatically generated

Answer the following questions:

* What is the SSIDs of the access point that is issuing beacon frames in this trace?
  + Wireshark-SAE
* What (in hexadecimal notation) is the MAC BSS id on the beacon frame?
  + 9c:d6:43:32:b9:f1
* What (in hexadecimal notation) is the destination MAC address on the beacon frame?
  + ff:ff:ff:ff:ff:ff
* The beacon frames from the access point advertise that the access point can support eight data rates and four additional “extended supported rates.” What are these rates?
  + Eight data rates: 1, 2, 5.5, 11, 6, 9, 12, 18; extended supported data rates: 24, 36, 48, 54

In RSN (Robust Security Network), there are three type of cipher suites  
1. Group Data Cipher Suite - protects group addressed frames which is used by BSS.  
2. Pairwise Cipher Suit List - a series of pairwise cipher suites.  
3. Group Management Cipher Suite - protects group addressed robust management frames which is used by BSS.

* RSN Information: What is the Authentication and Key management Suite (AKM), Group Cipher Suite and used here?
  + AKM suite: SEA (SHA256); GC suite: AES (CCM); GMC suite: AES (CCM)

**3. SAE handshake**

There are four data packets exchanged in this stage by the client and AP during which they send each other a Commit or ‘1’ and Confirm or ‘2’ messages. A group is selected and minimum ECDH-Group 19 support (256 bit) must be there for interoperability. Commit message containing Group ID, a Scalar & Finite Field Element (FFE) that is produced using PWE, which is generated by both sides prior to SAE, are exchanged between the client and AP via authentication frames. Answer the following questions based on these data packets:

* What (in hexadecimal notation) is the destination MAC address on the client?
  + 9c:d6:43:e7:bb:68
* What is the Group ID, a Scalar, element (FFE) and status code generated and sent by the client in the commit message?

Graphical user interface, text, application

Description automatically generated

* What is the Group ID, a Scalar, element (FFE) and status code generated and sent by the AP in the commit message?

Graphical user interface, text, application

Description automatically generated

* Check the parameters of the confirm authentication frames exchanged between client and AP respectively and indicate if they have successfully completed SAE handshake. Include screenshots.

Graphical user interface, text, application

Description automatically generated

**4. Association request and response**

During phase 2 of WPA3-SAE, association request and response messages are exchanged between client and the AP. Answer the questions below based on these data packets:

* Include screenshots to indicate successful association response sent by the AP to client.

Text

Description automatically generated

* What are the security parameters being agreed upon by client and AP?
  + AKM suites- SAE, group cipher suites

**5. 4-Way handshake**

AP and client go through 4-way handshake to derive keys to be used for secure data exchange. Answer the questions below based on these EAPOL data packets:

* What is the nonce sent by AP to the client? Hint: look at all the data packets sequentially.
  + 900bd25636a879752937f443bc2418c8191e5ba43e8f109fca96faedc1b4d2c9
* What is the nonce sent by the client to AP (this helps in generating shared keys)?
  + c7b1a41f2f4123715a391c660bdd66f89c4678674dd5919ab5cc1378c4048cd4
* What are the keys which get successively generated towards the end of 4-way handshake?
  + PTK, PMK, GTK
* Can you decrypt data packets now being exchanged in plain sight?
  + NO