April 2022

MULTI-FACTOR AUTHENTICATION IN WIRELESS NETWORKS

Sachin D. Wakudkar

Ugo Campiglio

MULTI-FACTOR AUTHENTICATION IN WIRELESS NETWORKS

AUTHORS:
Sachin D Wakudkar
Ugo Campiglio

ABSTRACT

Wireless networks employ many forms of single and multiple authentication techniques (many of which may be combined) to support both different types of devices and strong authentication methods. However, there are times when such strong methods may not be used (when, for example, devices such as Internet of things (IoT) devices, voice over Internet Protocol (VoIP) phones, etc. do not allow user input or the installation of a certificate) and a weaker method (such as a Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)) may be selected. In such cases, Multi-factor authentication (MFA), leveraging out-of-band (OOB) communication, could be employed to increase the authentication security level. Accordingly, techniques are presented herein that support a new method for wireless client authentication – which may be referred to herein as WPA-PSK + OOB authentication – that combines the easy configuration that is provided by a WPA-PSK with the strong authentication that is provided by an MFA infrastructure.

DETAILED DESCRIPTION

Currently, wireless networks employ numerous forms of single and multiple authentication methods, many of which may be combined. Among other things, wireless networks need to support both different types of devices and strong authentication methods (such as the Institute of Electrical and Electronics Engineers (IEEE) standard 802.1X). However, there may be times when such strong authentication methods cannot be used because some of the devices (such as Internet of things (IoT) devices, voice over Internet Protocol (VoIP) phones, etc.) may not allow user input or the installation of a certificate. As a result, many times a Wi-Fi Protected Access Pre-Shared Key (WPA-PSK) authentication method may be chosen. However, such a selection considerably reduces the authentication security level.

Multi-factor authentication (MFA) may be employed to increase the authentication security level in many applications and could also be used by wireless local area networks (WLANs) to improve security.

Using MFA combined with a WPA-PSK could take advantage of a simple Layer 2 (L2) authentication (where no certificate or user input are required on a device), but still provide a strong authentication method occurring out-of-band (OOB).

Accordingly, techniques are presented herein that support a new wireless authentication method – OOB authentication – that, among other things, leverages the already existing MFA infrastructure.

Figure 1, below, illustrates elements of MFA in a wireless network according to aspects of the techniques presented herein and reflective of the discussion that was presented above.

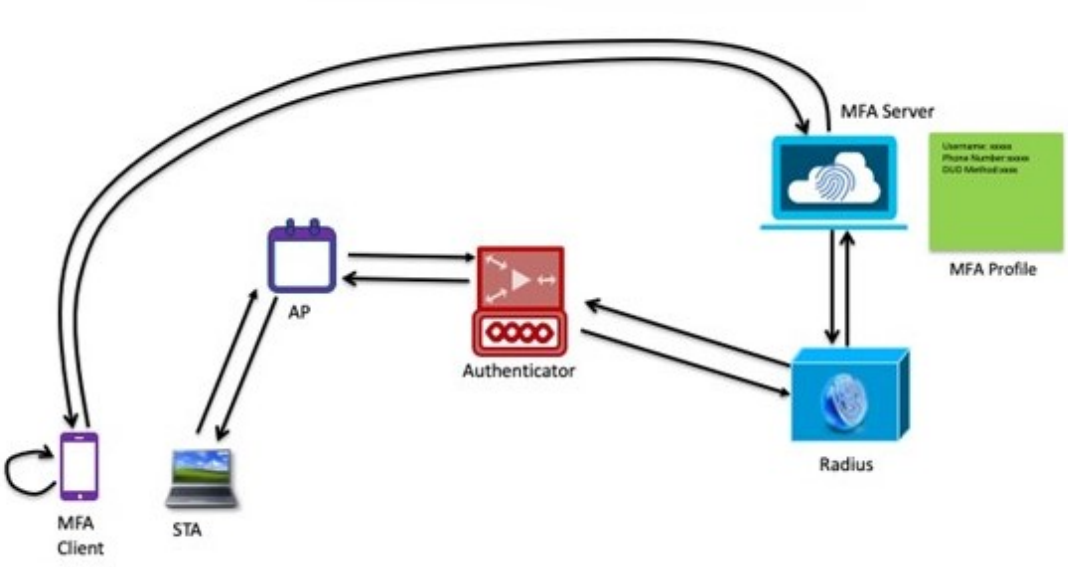

Figure 1: Exemplary MFA in a Wireless Network

As depicted in Figure 1, above, when a station (which is identified as STA in the figure) wishes to connect to a wireless network, MFA may be completed through the use of a preregistered user device (which is identified as MFA Client in the figure). The STA may associate with a new authentication method combining a Pre-Shared Key (PSK)(such as a shared passphrase) and OOB authentication (relying on the MFA infrastructure).

Figure 2, below, depicts elements of an exemplary sequence diagram, according to aspects of the techniques presented herein, for the new authentication method that was described above (which may be referred to herein as WPA-PSK + OOB authentication).

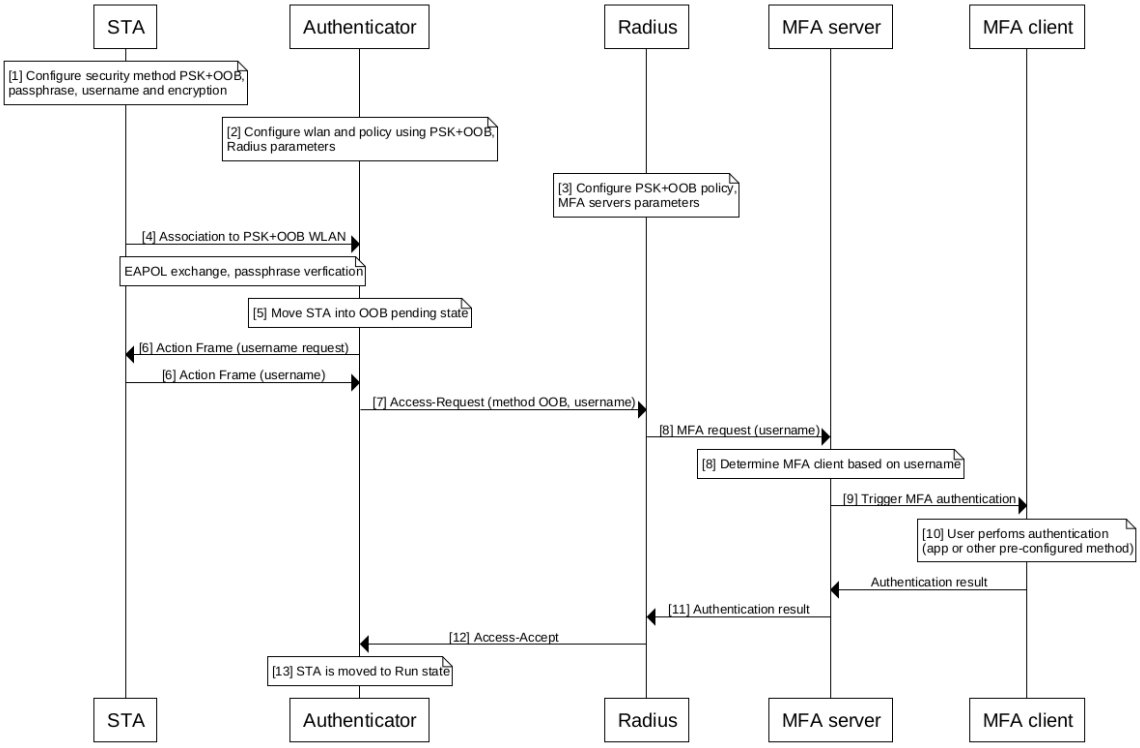

Figure 2: Sequence Diagram for WPA-PSK + OOB Authentication

The sequence diagram that is presented in Figure 2, above, identifies a series of steps. Those steps, which are labeled 1 through 13 in the figure, will be described below.

During Step 1, a user configures WPA-PSK + OOB authentication on their client (i.e., the supplicant) which is identified as STA in the figure. In addition to the PSK parameters, a username may also be entered. During Step 2, WPA-PSK + OOB authentication is selected as the WLAN security approach on the Authenticator, and, under Step 3, a Remote Authentication Dial-In User Service (RADIUS) policy is configured for the given WLAN to use MFA authentication. At Step 4, the client connects to the Authenticator and PSK authentication takes place. During Step 5, if PSK authentication is

successful then the client may be held in a new OOB Authentication Pending state. In such a state, the client can only send and receive Action Frames for delivering a userid.

During Step 6, the Authenticator retrieves the userid from the supplicant through dedicated Action Frames after which, at Step 7, the Authenticator sends an Access-Request (containing the userid) to the RADIUS server. The OOB authentication method may be known by the RADIUS server through rules that are configured for the WLAN (which is a preferred method). Alternatively, such information may be sent in an attribute-value pair (AVP) in the Access-Request.

During Step 8, the RADIUS server receives the request and sends the authentication request to the MFA server after which, at Step 9, the MFA server contacts the registered user MFA client based on the received userid. In the instant scenario, it is assumed that the userid as well as the method for performing the MFA are already known by the MFA server.

During Step 10, the user (through the MFA client) performs the MFA. At Step 11, the MFA server sends the authentication response to the RADIUS server where, at Step 12, the RADIUS server sends an Access-Accept or an Access-Reject to the Authenticator with a new AVP. Finally, at Step 13 the Authenticator allows the client to transition to a run state through which the client may now access the network.

Table 1, below, presents several new RADIUS AVPs according to aspects of the techniques presented herein and reflective of the above discussion.

Table 1: New RADIUS AVPs

Message Type	Attribute Type	Name/Key	Description
Access Request	Vendor-specific attribute (VSA)	Oob	Authentication method identifier
Access Request	VSA/Standard	Userid	String containing userid
Access Reject	Standard	WLAN Reason Code	New authentication failure reason code "MFA Unspecified Failure" and "MFA Timeout" having a format that is defined in Section 2.13 of the Internet Engineering Task Force (IETF) Request for Comments (RFC) 7268

Table 2, below, presents two new Institute of Electrical and Electronics Engineers (IEEE) technical standard 802.11 reason codes according to aspects of the techniques presented herein and reflective of the above discussion.

Table 2: New IEEE 802.11 Reason Codes

Name	Meaning
MFA_UNSPECIFIED_FAILURE	MFA failure either due to invalid method or token
MFA_NO_RESPONSE	Client not responding for a given timeout for MFA

As described and illustrated in the above narrative, the techniques presented herein employ MFA to provide for an increased security level, while still benefiting from the simple configuration of a PSK, by leveraging the existing wireless and MFA infrastructure during device authentication and without requiring any additional applications or tokens.

According to aspects of the techniques presented herein, the OOB authentication approach that was described above may be extended to other authentication methods that, for example, already employ a RADIUS server. For example, IEEE 802.1X (dot1x)-based or web-based authentication could increase their security level by adding an OOB authentication with the MFA infrastructure.

In connection with the techniques presented herein, it is important to note that an Authenticator-RADIUS exchange (as depicted in Figure 2, above) does not require any change. The RADIUS server requires that the WLAN profile be configured to perform an additional MFA step. Because MFA requires user input, the authentication will take a considerably longer time. As a result, this implies that the Authenticator timeout for a RADIUS response will need to be adjusted accordingly.

Further, media access control (MAC) Authentication Bypass (MAB) could also make use of the above-described OOB authentication mechanism. In such a case, it would be necessary to create a new database containing a device identifier, along with a user that is associated with same, so that the MFA server may determine (based on a device identifier) to which user the MFA process should be directed. A device identifier may be a device's MAC address or it may be some other identifier that is sufficiently robust in light of randomized changing MAC mechanisms.

In summary, techniques have been presented that support a new method for wireless client authentication – which may be referred to herein as WPA-PSK + OOB authentication – that combines the easy configuration that is provided by WPA-PSK with the strong authentication that is provided by an MFA infrastructure.