IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protect SSID in 4-way handshake | | | | |
| Date: 2024-05-16 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm Technologies, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

A paper (\*) describes issues with IEEE 802.11 not authenticating the SSID in all cases and some upper layer components using the current SSID to disable protections (e.g., disabling VPN in a trusted network). The paper describes a man-in-the-middle attack that allows a STA to be made to believe it associated with a different SSID when that STA has same credentials enabled for multiple SSIDs.

This contribution proposes an extension to the IEEE 802.11 standard to enable one of the mitigations proposed in the paper. This allows the SSID to be included in the protected 4-way handshake message 3 which allows the STA/Supplicant to verify that the SSID it believes the network to use is indeed the same SSID that the AP/Authenticator uses.

(\*) H. Gollier and M. Vanhoef. SSID Confusion: Making Wi-Fi Clients Connect to the Wrong Network. To appear in the *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2024.

The paper is publicly available before the conference at

https://www.top10vpn.com/research/wifi-vulnerability-ssid/

# Discussion

While some of the issues described in the paper could be mitigated with implementation changes and use of beacon protection, that approach is not ideal and has some practical limitations. A simple protocol extension can be used to provide a complete protection for this.

The paper section 5.2 proposes two potential protocol updates to avoid the issues. (1) mixing in SSID into key derivation for all cases and (2) include SSID in an authenticated frame. (2) seems to be significantly simpler approach and that is what is proposed here. This needs some additional consideration due to likely interoperability issues with almost any 4-way handshake change that would be done unconditionally, i.e., the AP and STA need to be able to determine that they support this new mechanism (and to do that in a manner that cannot be bypassed by an MITM attacker).

It should be noted FILS authentication and mesh AMPE might need additional changes. This contribution focuses in the more commonly used 4-way handshake cases to allow them to be discussed and addressed more quickly.

# Proposed text changes to IEEE P802.11REVme/D5.0

**9.4.2.240 RSNXE**

*Insert a new row into Table 9-373 immediately above the last Reserved row as shown below (ignoring the header row)*

**Table 9-373—Extended RSN Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | SSID protection | A STA indicates it supports protected exchange of the SSID during 4-way handshake. |

**12.7.4 EAPOL-Key PDU notation**

*Modify 12.7.4 as shown below (REVme/D5.0 P3101 L10)*

OCI KDE is the OCI KDE

RSNXE is the RSNXE, described in 9.4.2.240 (RSNXE)

PMKID is the PMK identifier for the PMKSA selected by the Authenticator

SSID is the SSID element, described in 9.4.2.2 (SSID element)

[a] means that a is optionally or conditionally present in {Key Data}

**12.7.6 4-way handshake**

**12.7.6.1 General**

*Modify 12.7.6.1 as shown below (REVme/D5.0 P3101 L50)*

RSNA defines a protocol using EAPOL-Key PDUs called the 4-way handshake. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator--> Supplicant: EAPOL-Key(0 or 1,0,1,0,P,0,0,ANonce,0,

{PMKID})

Message 2: Supplicant --> Authenticator: EAPOL-Key(0 or 1,1,0,0,P,0,0,SNonce,MIC,

{RSNE [, RSNXE]} [, OCI])

Message 3: Authenticator --> Supplicant:

EAPOL-Key(1,1,1,1,P,0,RSC,ANonce,MIC,{RSNE [, RSNXE] [, OCI].

GTK[N]} [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)] [, SSID]}

Message 4: Supplicant --> Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,{}).

**12.7.6.4 4-way handshake message 3**

*Modify 12.7.6.4 as shown below (REVme/D5.0 P3106 L56)*

Key Data =

...

* The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent.
* The SSID element containing the SSID of the BSS when both the Authenticator and the Supplicant have indicated support for SSID protection in the RSNXE.

**12.7.6.6 4-way handshake implementation considerations**

*Modify 12.7.6.6 as shown below (REVme/D5.0 P3109 L37)*

...

If the RSNE check for message 2 or message 3 fails, the SME should log an error and deauthenticate the peer.

The Authenticator and Supplicant shall check the Key Ack and Request bits in EAPOL-Key PDUs to stop reflection attacks.

The Supplicant shall not use message 1 contents to update state, in particular the keys in use, until validated with message 3.

If the Supplicant indicated support for SSID protection in its RSNXE and the Authenticator indicated support for SSID protection in its RSNXE, the Supplicant shall verify that the Key Data field in message 3 contains the SSID element and that the SSID indicated in that element bitwise matches the SSID indicated in the SSID element it used in the (Re)Association Request frame. If this verification fails, the Supplicant shall abondon the 4-way handshake and deauthenticate the peer.