### IEEE P802.11 Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Protected Password Identifiers for Privacy | | | | |
| Date: 2022-11-13 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
| Jouni Malinen | Qualcomm |  |  |  |
| Mike Montemurro | Huawei |  |  |  |

Abstract

This submission proposes a way to provide privacy protections to SAE password identifiers.

SAE password identifiers allow an ESS (identified by a single SSID) to support multiple passwords for access. These passwords can be given out on a per-STA basis or to a group of STAs that share common access permissions. It is possible to assign authorization policy—VLAN, ACLs, etc—to users based on the password identifier they used when authenticating.

Vendors have done similar per-user credential schemes with PSK mode. These schemes suffer from supporting a limited number of unique credentials and requirements for the AP to do a considerable amount of work to support the scheme. In spite of that, they are still popular. But these schemes do not work with SAE due to the forward secrecy properties of SAE. Password identifiers are the way to provide support for this use case with the enhanced security that SAE provides.

Unfortunately, SAE password identifiers are passed in the clear. This has caused certain large STA vendors to refuse to implement them in spite of them being extremely useful and solving legitimate use cases. This is causing a reluctance in certain markets to adopt stronger SAE authentication in favour of insecure PSK authentication in order to maintain the per-user credential capability.

To address the concerns of these large STA vendors, it is proposed to actually provide a way of providing a STA with a pseudonymous, and stateless identity that can be used for one-time access and a way to obtain a new pseudonym for use with a subsequent connection. This technique can scale to a large number of unique passwords and uses a minimum of computational overhead on the part of the AP.

This scheme has the following security properties:

* A passive attacker cannot determine a protected identity;
* Identifiers are protected against active attack insofar as SAE is resistant to active attack;
* A passive attacker cannot connect protected identities across distinct SAE protocol runs;
* Password identifiers can be arbitrarily padded to foil passive traffic analysis;
* Protected identities are secure under a birthday bound of 232 encryptions;
* An attacker cannot tamper with or substitute identifiers to connect distinct runs of SAE;
* An AP needs to only manage a single credential;
* APs in an ESS can share the single credential (in an out of band, out of scope manner);
* APs can use the same credential to protect all groups in the ESS that use password identifiers;
* Identities are protected against members of the same group;
* The interface for password identifiers on a STA is unchanged;
* The overhead is minimal—25 octets plus padding;
* Uses symmetric cryptography for speed and DOS resistance;
* Protected password identifiers in a mesh is supported.

The proposal can be implemented by accepting the following changes to Draft P802.11REVme\_2.0:

*Instruct the editor to modify section 9.3.3.11 as indicated:*

**9.3.3.11 Authentication frame format**

**Table 9-68—Authentication frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 22 | Password Identifier | The Password Identifier element is optionally present in certain Authentication frames as defined in Table 9-69 (Presence of fields and elements in Authentication frames) |
| 23 | Rejected Groups | The Rejected Groups element is present only in certain Authentication frames as defined in Table 9-69 (Presence of fields and elements in Authentication frames). |
| 24 | Anti-Clogging Token Container | The Anti-Clogging Token Container element is present only in certain Authentication frames as defined in Table 9-69 (Presence of fields and elements in Authentication frames). |
| 25 | AKM Suite Selector | The AKM Suite Selector element is present only in certain Authentication frames as defined in Table 9-69 (Presence of fields and elements in Authentication frames). |
| 26 | Protected Password Identifier | The Protected Password Identifier element is optionally present in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames). |
| Last | Vendor Specific | One or more Vendor Specific elements are optionally present. These elements follow all other elements. |

**Table 9-69—Presence of fields and elements in Authentication frames**

|  |  |  |  |
| --- | --- | --- | --- |
| Authentication algorithm | Authentication transaction sequence number | Status code | Presence of fields and elements from order 4 onwards |
| SAE | 1 | Any | The Scalar field is present if the Status Code field is zero or 126.  The FFE field is present if the Status Code field is zero or 126.  When the hunting-and-pecking method is used to drive the PWE, the Anti-Clogging Token field is present if the Status Code field is ANTI\_CLOGGING\_TOKEN\_REQUIRED or if the Authentication frame is in response to a previous rejection with the Status Code field equal to ANTI\_CLOGGING\_TOKEN\_REQUIRED.  The Finite Cyclic Group field is present if the Status Code field is zero, ANTI\_CLOGGING\_TOKEN\_REQUIRED, 77, or 126.  The Password Identifier element is optionally present if the Status Code field is zero, 123, or 126, and the Protected Password Identifier element is not present.  If the Status Code field is 126, the Rejected Groups element is conditionally present as described in 12.4.7.3 (Encoding and decoding of SAE Commit messages); otherwise the Rejected Groups element is not present.  The Rejected Groups element is present if the Status Code field is 126.  When the hash-to-element method is used to derive the PWE, the Anti-Clogging Token Container  element is present if the Status Code field is ANTI\_CLOGGING\_TOKEN\_REQUIRED or if the Authentication frame is in response to a previous rejection with the Status Code field equal to ANTI\_CLOGGING\_TOKEN\_REQUIRED.  If the Status Code field is 126, the Rejected Groups element is conditionally present as described in 12.4.7.3 (Encoding and decoding of SAE Commit messages); otherwise the Rejected Groups element is not present. When the hash-to-element method is used to derive the PWE, the Anti-Clogging Token Container element is present if the Status Code field is ANTI\_CLOGGING\_TOKEN\_REQUIRED or if the Authentication frame is in response to a previous rejection with the Status Code field equal to ANTI\_CLOGGING\_TOKEN\_REQUIRED. (M67)The AKM Suite Selector element is present if 00-0F-AC:24 or 00-0F-AC:25 is the intended AKM (see 12.4.5.3 (Construction of an SAE Commit message) and 12.4.5.4 (Processing of a peer’s SAE Commit message)); otherwise, it is not present.  The Protected Password Identifier element is optionally present if the Status Code field is zero, 123, or 126, and the Password Identifier field is not present. |

*Instruct the editor to modify table 9-128 as indicated, obtain a new identifier for the new element, and replace <ANA-1> with that number.*

**9.4.2 Elements**

**9.4.2.1 General**

**Table 9-128—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Element ID Extension** | **Extensible** | **Fragmentable** |
| Originator Preferred MCS (see 9.4.2.297 (Originator Preferred MCS element | 255 | 116 | Yes | No |
| Protected Password Identifier element (see 9.4.2.X (Protected Password Identifier element)) | 255 | <ANA-1> | No | No |
| Reserved | 255 | <ANA-1> + 1-255 |  |  |

*Instruct the editor to create a new section as below, replacing X with the appropriate number and assigning the figure number appropriately:*

**9.4.2.X Protected Password Identifier element**

The Protected Password Identifier element is used to convey a password identifier duing an authentication exchange in a manner that will hide the actual value from attackers. The format of the Protected Password Identifier element is shown in Figure 9-XYZ (Protected Identifier element format).

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID  Extension | Protected Identifier |

Octets: 1 1 1 variable

**Figure 9-XYZ—Protected Identifier element format**

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1 (General).

The Protected Identifier field contains an opaque variable-length string.

*Instruct the editor to modify section 9.6.15.3.2 as indicated:*

**9.6.15.3.2 Mesh Peering Confirm frame details**

**Table 9-520—Mesh Peering Confirm frame Action field format**

|  |  |  |
| --- | --- | --- |
| Order | Information | Notes |
| 18 | HE Capabilities | The HE Capabilities element is present when dot11HEOptionImplemented is true; otherwise, it is not present. |
| 19 | HE Operation | The HE Operation element is present when dot11HEOptionImplemented is true; otherwise, it is not present. |
| 20 | Protected Password Identifier | The Protected Password Identifier element is optionally present if a mesh STA wishes to provide a protected password identififer to a peer mesh STA |

*Instruct the editor to modify section 12.4.3 as indicated:*

**12.4.3 Representation of passwords and password identifiers**

In an infrastructure BSS for which an SAE AKM is indicated, the AP shall set the SAE Password Identifiers In Use subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if any entry in the dot11RSNAConfigPasswordValueTable has a non-NULL dot11RSNAConfigPasswordIdentifier, and shall set it to 0 otherwise. Similarly, an AP shall set the SAE Password Identifiers Used Exclusively subfield of the Extended Capabilities field of the Extended Capabilities element to 1 if every entry in the dot11RSNAConfigPasswordValueTable has a non- NULL dot11RSNAConfigPasswordIdentifier and shall set it to 0 otherwise.

After an initial connection with a plaintext password identifier, an AP (in an infrastructure BSS) or a mesh STA (in a mesh) can provide an encrypted identifier to the STA (infrastructure) or peer mesh STA (mesh), respectively, to use in a subsequent connection. The password identifier from the dot11RSNAConfigPasswordValueTable remains unchanged but the AP, or mesh STA, encrypts the identifier and sends the encrypted identifier to the STA (infrastructure) during the 4-way Handshake or peer mesh STA (mesh) during the AMPE. Each time an encrypted identifier is used in a subsequent SAE authentication it should be changed for the next authentication using the technique described here such that each encrypted identifier is used with only one run of the SAE protocol.

Support for protected password identifiers is done on an entire ESS basis, such that if a non-AP STA receives a protected password identifier from one AP it will be supported and understood by other APs in the ESS.

1. An AP or mesh STA that supports protected password identifiers shall generate a secret to use with AES-SIV (either a 256-bit or 512-bit key), referred to as *pk* below. The encrypted identifier shall be generated as follows, given a plaintext password identifier:The plaintext password identifier shall be pre-pended with 1 or more octets of padding, the first of which indicates the length of the pad—e.g. if there are 4 octets of padding then the sequence would be 4-0-0-0, if there is only one octet of padding the sequence would simply be 1—the length of the pad should vary each time an encrypted identifier is generated;
2. An 8 octet random string, denoted here as *s*, is generated and prepended to the padded plaintext identifier to produce a string denoted here *p*;
3. A ciphertext, *c*, is generated using AES-SIV in deterministic mode (no AAD), *pk* as the key, and *p* as the plaintext;
4. *c* becomes the encrypted identifier.

The encrypted identifier is provided to a STA in an infrastructure BSS in message 3 of the 4 Way Handshake in the PPI KDE (see 12.7.2), and provided to a peer mesh STA in a mesh in a Mesh Peering Confirm frame (see 14.5.5.3.1) in the Protected Password Identifier element (see 9.4.2.X).

A STA or mesh STA that receives an encrypted identifier shall retain it and shall use it in a subsequent SAE authentication to another AP in the ESS (infrastructure) or another mesh STA (mesh).

When a STA or mesh STA uses an encrypted identifier in SAE it shall pass it in the Protected Password Identity element in an SAE Commit message. When the Protected Password Identifier element is present in an SAE Commit message, the Password Identifier element shall not be present.

When an AP or mesh STA receives a Protected Password Identifier element in an SAE Commit message it shall decrypt the identity as follows, using the Protected Identifier from the Protect Password Identifier element as *c*:

1. A plaintext, *p*, is generated by decrypting using AES-SIV in deterministic mode (no AAD), *pk* as the key and *c* as the ciphertext;
2. The first 8 octets—the random string *s*—are removed from *p* and discarded;
3. The length of the pad, *t*, is determined from first of the remaining octets of *p*;
4. The first *t* octets of *p* are removed and the remainder is the decrypted password identifier.
5. If AES-SIV decryption fails, SAE authentication fails.

*Instruct the editor to modify section 12.4.4.2.3 as indicated:*

**12.4.4.2.3 Hash-to-element generation of the password element with ECC groups**

The SSWU method produces two values, x1, and x2, at least one of which will represent an abscissa of a point on the curve. If x1 is the abscissa, then x1 becomes the x-coordinate otherwise x2 becomes the x-coordinate. The equation of the curve with the x-coordinate produces the square of the y-coordinate which is recovered by taking the square root. The two possible results of the square root are discriminated by checking its least significant bit with the least significant bit of u. The result is a point on the curve.

The *identifier* used in the calculations above shall be the value extracted from the SAE Commit message. If protected password identifiers are used, the identifier in the calculations above shall be the encrypted value from the Protected Identifier field of the Protected Password Identifier element, otherwise it shall be the value from the Identifier field of the Password Identifier element.

*Instruct the editor to modify section 12.4.4.3.3 as indicated where the deleted duplicative text occurs immediately before a formula for calculation of PT (formula in between the text is not shown):*

**12.4.4.3.3 Direct generation of the password element with FFC groups**

This secret PT is stored until needed to generate a session specific PWE (see 12.4.5.2 (PWE and secret generation)).

The *identifier* used in the calculations above shall be the value extracted from the SAE Commit message. If protected password identifiers are used, the identifier in the calculations above shall be the encrypted value from the Protected Identifier field of the Protected Password Identifier element, otherwise it shall be the value from the Identifier field of the Password Identifier element.

*Instruct the editor to modify section 12.4.5.4 as indicated:*

**12.4.5.4 Processing of a peer’s SAE Commit message**

If the peer’s SAE Commit message contains a password identifier, the value of that identifier shall be used in construction of the password element (PWE) for this exchange. If the peer’s SAE Commit message contains an encrypted identifier, the encrypted identifier shall be used in construction of the secret element PT for this exchange (see 12.4.4.2.3 (Hash-to-element generation of the password element with ECC groups) and 12.4.4.3.3 (Direct generation of the password element with FFC groups). If peer privacy is supported, an encrypted identifier shall be generated from the plaintext password identifier (see 12.4.3 (Representation of passwords and identifiers)) and transmitted to the peer in the 4 Way Handshake (for an Infrastructure BSS) or AMPE (for a mesh STA) after SAE has successfully terminated. If a password identifier, or protected password identifier, is present in the peer’s SAE Commit message and there is no password with the given (decrypted) identifier a STA shall fail authentication.

*Instruct the editor to obtain a new data type from ANA and modify table 12-10 in section 12.7.2 as indicated, replacing <ANA-2> below with the new data type:*

**Table 12-10—KDE selectors**

|  |  |  |
| --- | --- | --- |
| **OUI** | **Data type** | **Meaning** |
| 00-0F-AC | 13 | OCI KDE |
| 00-0F-AC | 14 | BIGTK KDE |
| 00-0F-AC | 15 | WIGTK KDE |
| 00-0F-AC | <ANA-2> | PPI KDE |
| 00-0F-AC | <ANA-2>+1-255 | Reserved |
| Other OUI or CID | Any | Vendor specific |

*Instruct the editor to append the following to section 12.7.3 assigning a figure number as appropriate:*

The format of the PPI KDE is shown in Figure 12-AB (PPI KDE).

|  |
| --- |
| PPI |

Octets: (Length – 4)

**Figure 12-AB—PPI KDE format**

The PPI is an opaque string that shall be retained by a STA and used as a Protected Password Identifier with a subsequent SAE authentication to the same ESS with which it is performing the 4-way Handshake.

*Instruct the editor to modify section 12.7.6.4 as indicated:*

**12.7.6.4 4-way handshake message 3**

Key Data =

* For PTK generation for the current operating band, the AP’s Beacon/Probe Response frame’s RSNE for the current operating band, and, optionally, a second RSNE that is the Authenticator’s pairwise cipher suite assignment for the current operating band, and, if a group cipher has been negotiated, the GTK and the GTK’s key identifier (see 12.7.2 (EAPOL-Key frames)) for the current operating band, and if management frame protection is negotiated, the IGTK KDE, and if beacon protection is enabled, the BIGTK KDE(11ba), and if WUR frame protection is negotiated, the WIGTK KDE, and if protected password identifiers are supported, the PPI KDE, and when this message 3 is part of a fast BSS transition initial mobility domain association or an association started through the FT protocol, the PMKR1Name calculated according to the procedures of 12.7.1.6.4 (PMK-R1) in the PMKID List field of the RSNE and the FTE with the same contents as in the (Re)Association Response frame, the MDE with the same contents as in the (Re)Association Response frame, the reassociation deadline timeout set to the minimum of dot11FTReassociationDeadline and the key lifetime in the TIE[ReassociationDeadline], and the PTK lifetime in the TIE[KeyLifetime]; or

*Instruct the editor to modify section 14.5.5.3.1 as indicated:*

**14.5.5.3.1 Generating Mesh Peering Confirm frames for AMPE**

In addition to contents for establishing a mesh peering as specified in 14.3.7.1 (Generating Mesh Peering Confirm frames), the Mesh Peering Confirm frame, when used with the AMPE, shall contain the following:

* In the Mesh Peering Management element, the Mesh Peering Protocol Identifier shall be set to 1 “authenticated mesh peering exchange protocol.”
* The RSNE shall be the same as sent in the Mesh Peering Open frame.
* If the PMK used in the AMPE exchange was generated using SAE and the mesh STA wishes to supply the peer mesh STA with a protected identifier, the Protected Password Identifier element shall be present. The Protected Identifier field shall be constructed per 12.4.3 (Representation of passwords and password identifiers).
* In the Authenticated Mesh Peering Exchange element:
  + The Selected Pairwise Cipher Suite field shall be set to the cipher suite selector that indicates the successfully selected pairwise cipher suite (specified in 14.5.2.1 (Instance Pairwise Cipher Suite selection)).
  + The Peer Nonce field shall be set to the nonce value chosen by the peer mesh STA as received in the Local Nonce field in the Mesh Peering Open frame from the candidate peer mesh STA.
  + The GTKdata field shall not be present.
  + The IGTKdata field shall not be present.
  + The rest of fields are set to the same values sent in the Mesh Peering Open frame.

The Mesh Peering Confirm frame shall be protected using AES-SIV as specified in 14.5.3 (Construction and processing AES-SIV-protected mesh peering Management frames). **References:**