IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Finding PWE in Constant Time | | | | |
| Date: 2019-07-08 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott boulevard  Santa Clara, California,  United States of America | +1 408 555 1212 |  |
|  |  |  |  |  |

Abstract

The countermeasures against side channel attack that SAE puts into the hunting and pecking loop is inefficient and fragile. Recent attacks—e.g. Dragonblood—underscore this problem. PWE should be discovered in a deterministic method which is computable in constant time without repetitive looping. Do to the minimal number of restrictions on curve type, an appealing way of hashing to an elliptic curve is the Shallue-Woestijne-Ulas (SWU) method. For FFC groups, the branching and looping should be removed in order to generate an FFC PWE directly. In addition, it’s important to add detection of group downgrade to SAE.

**Discussion**: SAE requires use of a secret element, PWE, discovered in an agreed upon finite cyclic group. Due to the way the key exchange was initially developed this PWE discovery cannot be done before the SAE protocol starts.

This element is deterministically discovered by repeatedly hashing the password with some additional information until the resulting hash is the abscissa of a point on the elliptic curve (for ECC) or by exponentiating the hash digest to a constant to produce an element (for FFC). Both of these techniques are prone to side channel attack. While much work has gone into countermeasures to mitigate these attacks, for instance looping 40 times regardless of how soon an abscissa is found, the countermeasures render the whole method of PWE discovery inefficient and very fragile.

When a group is rejected another one is tried. A man-in-the-middle could exploit this to do a downgrade attack where “good” groups are rejected by the attacker until a “not so good” group is offered which is allowed to go through. There is no way to detect this attack.

**Proposal**: For ECC, use the Shallue-Woestijne-Ulas (SWU) to directly hash-to-curve. This method will work for any Weierstrass curve which makes it ideal for use with SAE.

Since SWU does not generate all points on the elliptic curve, the SWU method by itself could not be used with the current SAE security proof in the random oracle model. Therefore, the SWU method is enhanced by the following technique from Brier et al to hash to a password-based element, PT:

PT(m) := SWU(h1(m)) + h2(m) \* G

Where *m* is the information being hashed, *h1*() and *h2*() are random oracles based on a hash function, G is the generator of the curve being hashed into, ‘+’ is the element operator (i.e. point arithmetic) for ECC, and ‘\*’ is the scalar operator for ECC.

For FFC groups the results of the hash will be reduced module the prime to produce PT instead of skipping values which would be larger than the prime when interpreted as an integer. No looping is needed.

The secret element, PT, can be computed when the password is provisioned and retained until SAE begins at which time it can be combined with the peer’s MAC addresses to create a session-specific PWE for SAE.

Such an approach not only allows for hashing-to-element to be implemented in constant time but also avoids timing attacks for implementations that cannot be completely constant time.

These new techniques are not backwards compatible with the “hunting-and-pecking” loop in the standard and therefore must be signalled as new capabilities. This signalling is compounded by two things: SAE happens before association, and selection of PWE happens before any transactional frames have been sent. Since SAE happens before association, it’s not possible to use an AKM. So support of this is signalled by an AP using a bit in the Extended Capabilities field. Since the SAE protocol itself is not being changed the signalling to use this new PWE discovery method has to be as unintrusive as possible. Therefore, it is signalled with a new status code in the SAE Commit message—“I’m hashing directly to PWE!”. Everything else in SAE (state machine, message formats, computation, message construction and processing, etc) remains the same.

To detect a group downgrade, each peer appends rejected groups to its next Commit message. A concatenation of both sides’ lists of rejected groups (one or both can, of course, be null) is passed as salt to the key derivation function. This ensures that both sides will agree on the same key if there is no man-in-the-middle fiddling with SAE Commit messages. If there is a man-in-the-middle the SAE exchange will fail.

**Changes necessary:**

*Instruct the editor to add the following line to section 2:*

**2. Normative references**

IETF RFC 5869, HMAC-based Extract and Expand Key Derivation Function, H. Krawczyk, P. Eronen May 2010

*Instruct the editor to modify table 9-42 as indicated:*

**Table 9-42—Authentication frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| 23 | Rejected Groups | The Rejected Groups element is conditionally present in certain Authentication frames as defined in Table 9-43 (Presence of fields and elements in Authentication frames) |

*Instruct editor to modify table 9-43 as indicated:*

**Table 9-43—Presence of fields and elements in Authentication frames**

|  |  |  |  |
| --- | --- | --- | --- |
| **Authentication Algorithm** | **Authentication transaction sequence number** | **Status Code** | **Presence of fields 4 onwards** |
| SAE | 1 | Any | Scalar is present if the Status Code field is zero or 124.  Element is present if the Status Code field is zero or 124.  Anti-Clogging Token is present if status is 76 or if  frame is in response to a previous rejection with Status 76.  Finite Cyclic Group is present if the Status Code field  is zero,76, or 124.  Password Identifier element is optionally present  if the Status Code is zero, 123, or 124.  Rejected Groups element is contitionally present if the Status Code is 124. |

*Instruct the editor to modify table 9-52 as indicated:*

**Table 9-52—Status codes**

|  |  |  |
| --- | --- | --- |
| **Status code** | **Name** | **Meaning** |
| 124 | SAE\_HASH\_TO\_PWE | SAE authentication uses an alternate form of direct hashing, as opposed to looping, to obtain the PWE |
| 125 | REJECT\_MITM | Rejection of authentication due to detection of a man-in-the-middle attack |
| 126-65535 | Reserved |  |

*Instruct the editor to modify table 9-94 as indicates:*

**Table 9-94—Element IDs**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Element** | **Element ID** | **Extended ID Extension** | **Extensible** | **Fragmentable** |
| Rejected Groups (see 9.4.2.244 (Rejected Groups element)) | 255 | 90 | No | No |
| Reserved | 255 | 91-255 |  |  |

*Instruct the editor to modify table 9-95 as indicated:*

**Table 9-95—BSS membership selector value encoding**

|  |  |  |
| --- | --- | --- |
| **Value** | **Feature** | **Interpretation** |
| 123 | SAE Hash Only | Indicates that support for the direct hashing to element technique in SAE is required in order to join the BSS. |

*Instruct the editor to modify table 9-322 as indicated:*

**Table 9-322—Extended RSN Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| 5 | SAE hash-to-element | The AP supports directly hashing to obtain PWE instead of looping. See 12.4.4.2.3 and 12.4.4.3.3 |
| 6 – (8xn – 1) | Reserved |  |

*Instruct the editor to add new section 9.4.2.244, and allocate a number to replace XYZ, adjusting subsequent figure numbers as appropriate:*

**9.4.2.244 Rejected Groups element**

The Rejected Groups element lists the finite cyclic groups that have been rejected by a peer for use in SAE. The format of the Rejected Groups element is shown in Figure 9-XYZ

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Rejected Groups |

Octets: 1 1 1 variable

**Figure 9-XYZ—Rejected Groups element format**

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

The Rejected Groups field contains a concatenated list of unsigned integers representing Finite Cyclic Groups that have been rejected by a peer in a previous Authentication attempt.

*Instruct the editor to modify section 12.4.4.2.2 as indicated:*

**12.4.4.2.2 Generation of the password element with ECC groups by looping**

When a direct form of hashing to discover PWE is not signaled by the AP, or if the SAE initiator does not signal its use in its SAE Commit message, the password element of an ECC group (PWE) shall be generated in the following random hunt-and-peck fashion.

*Instruct the editor to add the following new section:*

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

An SAE peer, e.g. a Mesh STA or an AP, indicates support for direct hashing to obtain an ECC password element by setting the SAE hash-to-element bit in the Extended RSN Capabilities field in all Beacons and Probe Response frames. An SAE initiator that has identified a peer that supports this technique (through receipt of Beacons or Probe Response frames) shall derive a secret element, PT, according to the following technique and indicate this by setting the Status in the SAE Commit message to “SAE\_HASH\_TO\_ELEMENT”. An SAE initiator shall not indicate support for this form of element derivation unless its peer has already signalled support for this method. If an SAE Commit message is received with status equal to “SAE\_HASH\_TO\_ELEMENT” the peer shall generate PWE using the following technique and reply with its own SAE Commit message with Status equal to “SAE\_HASH\_TO\_ELEMENT.”

The direct hashing technique to derive an element of an ECC group is an enhancement of the deterministic hash-to-curve method Shallue-Woestijne-Ulas (SWU). It uses a construct of two distinct functions to produce two points on the elliptic curve. The two points are summed to create a secret element PT.

This hash-to-curve method uses HKDF (RFC 5869) with the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors)) to perform both functions. First HKDF-Extract is passed and all zero salt, the password, and optionally a password identifier to produce and intermediary password seed. The resulting seed is passed to HKDF-Expand to produce three distinct strings using different labels. The first value is reduced such that 0 < pwd-value < q, exclusive. That value is then uses as the scalar with the generator of the group in scalar-op() to produce a point on the curve, P1. The final two values are reduced such that 1 < pwd-value < p, exclusive and they are used, as *u* and *v*, with the SWU method to produce three values, x1, x2, and x3, at least one of them will represent an abscissa of a point on the curve. If x1 is the abscissa then x1 becomes the x-coordinate otherwise if x2 is the abscissa then x2 becomes the x-coordinate, otherwise x3 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 P2. PT is then the sum of the two points, PT = elem-op(P1, P2).

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

Algorithmically, this process is as follows:

*pwd-seed = HKDF-Extract(0n, password [|| identifier])*

*pwd-value = HKDF-Expand(pwd-seed, “SAE Hash to Element P1”, olen(p))*

*w = (pwd-value modulo (q-1)) + 1*

*P1 = scalar-op(w, G)*

*pwd-value = HKDF-Expand(pwd-seed, “SAE Hash to Element P2 u”, olen(p))*

*u = (pwd-value modulo (p-2)) + 2*

*pwd-value = HKDF-Expand(pwd-seed, “SAE Hash to Element P2 v”, olen(p))*

*v = (pwd-value modulo (p-2)) + 2*

*x1 = v*

*gx1 = x13 + a \* x1 + b modulo p*

*x2 = (-b/a) \* (1 + 1/(u4 \* gx12 + u2 \* gx1 ) modulo p*

*gx2 = x23 + a \* x2 + b modulo p*

*x3 = u2 \* gx1 \* gx2*

*gx3 = x33 + a \* x3 + b modulo p*

*l = gx2 is a quadratic residue modulo p*

*x = CSEL(l, x2, x3)*

*z = CSEL(l, gx2, gx3)*

*l = gx1 is a quadratic residue modulo p*

*x = CSEL(l, x1, x)*

*z = CSEL(l, gx1, z)*

*y = sqrt(z)*

*l = CEQ(LSB(u), LSB(y))*

*P2 = CSEL(l, (x,y), (x,p-y))*

*PT = elem-op(P1, P2)*

where

* HKDF-Extract() and HKDF-Expand are the functions defined in RFC 5869 instantiated with the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors))
* 0n represents a *salt* of all zeros whose length is the length of the digest of the instantiated hash function
* olen() returns the length of its argument in octets
* [|| identifier] indicates the optional inclusion of a password identifier, if present.
* G, p, q, a, and b are all defined in the domain parameter set for the curve.
* LSB(x) returns the least-significant-bit of x
* CSEL(x,y,z) operates in constant time and returns y if x is true and z otherwise.
* CEQ(x,y) operates in constant time and returns true if x equals y and false otherwise.

All operatioins shall be done in constant time. Implementations of this modified SWU method shall use the blinding technique from 12.4.4.2.2 to determine a quadratic residue.

Note—For curves based on a prime, p, such that p = 3 mod 4 the square root can be implemented with a single modular exponentiation of (p+1)/4, that is sqrt(w) = w(p+1)/4 modulo p.

*Instruct the editor to modify section 12.4.4.3.2 as indicated:*

**12.4.4.3.2 Generation of the password element with FFC groups by looping**

When a direct form of hashing to discover a password element is not signaled by the AP, or if the SAE initiator does not signal its use in the SAE Commit message the password element of an FFC group (**PWE**) shall be generated in the following random hunt-and-peck fashion.

*Instruct the editor to add the following new section:*

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

An SAE peer indicates support for direct hashing to obtain the FFC password element by setting the SAE hash-to-PWE bit in the Extended RSN Capabilities field in all Beacons and Probe Response frames. An SAE initiator that has identified a peer that supports the following technique (through receipt of Beacons or Probe Response frames) shall derive PT according to the following technique and indicate this by setting the Status in the SAE Commit message to “SAE\_HASH\_TO\_ELEMENT”. An SAE initiator shall not indicate support for this form of PWE derivation unless its peer has already signalled support. If an SAE Commit message is received with status equal to “SAE\_HASH\_TO\_ELEMENT” the peer shall generate PWE using the following technique and reply with its own SAE Commit message with Status equal to “SAE\_HASH\_TO\_ELEMENT.”

To perform this direct hashing technique, HKDF (RFC 5869) is passed a constant salt, the password, optionally a password identifier, as an input key, a constant label “SAE Hash to Element”, and the length of the prime to produce a password value. The resulting password value shall be reduced into a range such that 1 < pwd-value < p. Then, it shall be raised to the power (p–1) / q and reduced modulo p (where *p* is the prime number and *q* is the order). This will ensure PT is a generator of order either 1 (if PT=1) or q (for all other values). The probability of PT taking the value 1 is negligible.

This secret PT is stored until needed to generate a session-specific PWE.

Algorithmically, this process is as follows:

*pwd-value = HKDF(0n, password [|| identifier ], “SAE Hash to Element”, olen(p) )*

*pwd-value = (pwd-value modulo (p-2)) + 2*

*PT = pwd-value(p-1)/q modulo p*

where

* HKDF() is the function defined in RFC 5869 instantiated with the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors))
* 0n represents a *salt* of all zeros whose length is the length of the digest of the instantiated hash function
* olen() returns the length of its argument in octets
* [|| identifier] indicates the optional inclusion of a password identifier, if present.
* p and q are defined in the domain parameter set for the group.

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

*Instruct the editor to modify section 12.4.5.2 as indicated:*

**12.4.5.2 PWE and secret generation**

Prior to beginning the protocol message exchange, the secret element PWE and two secret values are generated.

When a STA supports a direct form of hashing to a group element (according to 12.4.4.2.3 or 12.4.4.3.3) it computes a secret element, PT, off-line at provisioning time for all groups it wishes to support with that password. Prior to initiating SAE to a STA which also supports the direct form of hashing to a group element, or upon receipt of an SAE Commit message indicating it was generated using a direct form of hashing to a group element, it shall generate PWE by hashing the two peer MAC addresses to produce a digest, reducing the digest modulo the order of the particular group, q, interpreting the reduced digest as an integer and using it with the secret element to generate PWE:

*val = H(MAX(STA-A-MAC, STA-B-MAC) || MIN(STA-A-MAC, STA-B-MAC))*

*val = val modulo (q – 1) + 1*

*PWE = scalar-op(val, PT)*

If a STA does not support a direct form of hashing to a group element it generates PWE after selecting a group , either the most preferred group if the STA is initiating SAE to a peer, or the group from a received SAE Commit message if the STA is responding to a peer. The PWE shall be generated for that group (according to 12.4.4.2.2 (Generation of the password element with ECC groups) or 12.4.4.3.2 (Generation of the password element with FFC groups), depending on whether the group is ECC or FFC, respectively) using the identities of the two STAs and the configured password.

After generation of the PWE, each STA shall generate a secret value, rand, and a temporary secret value, mask, each of which shall be chosen randomly such that 1 < rand < q and 1 < mask < q and (rand + mask ) mod q is greater than 1, where q is the (prime) order of the group. If their sum modulo q is not greater than 1, they shall both be irretrievably deleted and new values shall be randomly generated. The values rand and mask shall be random numbers produced from a quality random number drawn from a uniform distribution generator. These values shall never be reused on distinct protocol runs.

*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 a password identifier is present in the peer’s SAE Commit message and there is no password with the given identifier a STA shall fail authentication.

If the peer’s SAE Commit message contains a Rejected Groups element, the list of rejected groups shall be checked to ensure that all of the groups in the list are not approved groups. If any groups claimed to have been rejected are acceptable then then processing of the SAE Commit message fails and the STA shall reject the peer’s authentication with a status of REJECT\_MITM.

Upon receipt of a peer’s SAE Commit message both the scalar and element shall be verified.

If the scalar value is greater than 1 and less than the order, r , of the negotiated group, scalar validation succeeds; otherwise, it fails. Element validation depends on the type of group. For FFC groups, the element shall be an integer greater than 1 and less than the prime number p minus 1, (p – 1), and the scalar operation of the element and the order of the group, r , shall equal 1 modulo the prime number p . If either of these conditions does not hold, element validation fails; otherwise, it succeeds. For ECC groups, both the x- and y-coordinates of the element shall be non-negative integers less than the prime number p, and the two coordinates shall produce a valid point on the curve satisfying the group’s curve definition, not being equal to the “point at the infinity.” If either of those conditions does not hold, element validation fails; otherwise, element validation succeeds.

If either scalar validation or element validation fails, the STA shall reject the peer’s authentication. If both the scalar and element from the peer’s SAE Commit message are successfully validated, a shared secret element, K , shall be derived using the scalar and element (peer-commit-scalar and ***PEER-COMMITELEMENT*** , respectively) from the peer’s SAE Commit message and the STA’s secret value.

***K*** = scalar-op(rand , (elem-op(scalar-op(peer-commit-scalar , ***PWE***),

***PEER-COMMIT-ELEMENT***)))

If the shared secret element, ***K***, is the identity element for the negotiated group (the value one for an FFC group or the point-at-infinity for an ECC group) the STA shall reject the peer’s authentication. Otherwise, a secret value, k , shall be computed as:

k = F(K )

The entropy of k shall then be extracted using H to produce keyseed. The key derivation function from 12.7.1.6.2 (Key derivation function (KDF)) shall then be used with the hash algorithm identified by the AKM suite selector (see Table 9-151 (AKM suite selectors)) to derive a key confirmation key, KCK, and a pairwise master key, PMK, from keyseed. When used with AKMs 8 or 9, both the KCK and PMK shall be 256 bits in length, and therefore the length of keying material derived is 512. Use of other AKMs require definition of the lengths of the KCK, and the PMK. When both SAE Commit messages indicated a status of SAE\_HASH\_TO\_ELEMENT a salt is passed to the KDF consisting of a concatenation of the Rejected Groups from each peer’s Rejected Groups element, those of the peer with the highest MAC address go first (if only one sent a Rejected Groups element then the salt will consist of that list). If neither peer sent a Rejected Groups element or the status was not SAE\_HASH\_TO\_ELEMENT the salt shall consist of 32 octets of the value zero.

*keyseed = H(salt, k)*

*kck\_and\_pmk = KDF-Hash-512(keyseed, “SAE KCK and PMK”,*

*(commit-scalar + peer-commit-scalar) mod r)*

*KCK = L(kck\_and\_pmk, 0, 256)*

*PMK = L(kck\_and\_pmk, 256, 256)*

Where

* *salt* is either 32 octets of 0 or a list of rejected groups.
* *KDF-Hash-512* is the key derivation function defined in 12.7.1.6.2 (Key derivation function (KDF)) using the hash algorithm defined by the AKM suite selector (see Table 9-151 (AKM suite selectors)).

*Instruct the editor to modify section 12.4.7.4 as indicated:*

**12.4.7.4 Encoding and decoding of SAE Commit messages**

An SAE Commit message shall be encoded as an Authentication frame with an Authentication Algorithm

Number field set to 3, a Transaction Sequence Number of 1 and a Status Code of SUCCESS or SAE\_HASH\_TO\_ELEMENT. Status codes not equal to SUCCESS or SAE\_HASH\_TO\_ELEMENT indicate a rejection of a peer’s SAE Commit message and are described in 12.4.7.6 (Status codes).

An SAE Commit message shall consist of a Finite Cyclic Group field (9.4.1.42 (Finite Cyclic Group field)) indicating a group, a Scalar field (9.4.1.39 (Scalar field)) containing the scalar, and an FFE field containing the element (9.4.1.40 (FFE field)). If the SAE Commit message is in response to an Anti-Clogging Token field request (see 12.4.7.6 (Status codes)), the Anti-Clogging Token field is present (see 9.4.1.38 (Anti-Clogging Token field)). If a password identifier is used in generation of the password element (PWE) the Password identifier element shall be present and the identifier shall be encoded as a UTF-8 string in the Identifier portion of the element (see 9.4.2.216 (Password Identifier element)). If an SAE Commit message is being sent in response to rejection of a previous Commit message due to UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, the group that was rejected shall be appended, after the rejected groups from previous attempts if applicable, to the Rejected Groups portion of the Rejected Groups element.

*Instruct the editor to modify section 12.4.7.6 as indicated:*

**12.4.7.6 Status codes**

An SAE Commit message with a status code not equal to SUCCESS or SAE\_HASH\_TO\_ELEMENT shall indicate that a peer rejects a previously sent SAE Commit message. An unsupported finite cyclic group is indicated with a status code of UNSUPPORTED\_FINITE\_CYCLIC\_GROUP, “Authentication is rejected because the offered finite cyclic group is not supported.” An unknown password identifier is indicated with a status code of UNKNOWN\_PASSWORD\_IDENTIFER, “Authentication is rejected because the password identifier is unknown.” An Anti-Clogging Token field is requested by transmitting an SAE Commit message with a status code of ANTI\_CLOGGING\_TOKEN\_REQUIRED, “Anti-Clogging Token Requested,” with the Anti-Clogging Token field occupying the Token field of the Authentication frame.

**References:**

Brier E., Coron JS., Icart T., Madore D., Randriam H., Tibouchi M. (2010) “Efficient Indifferentiable Hashing into Ordinary Elliptic Curves.” In: Rabin T. (eds) Advances in Cryptology – CRYPTO 2010. Lecture Notes in Computer Science, vol 6223. Springer, 2010

Shallue, A. and van de Woestijne, C, “Construction of rational points on elliptic curves over finite fields”, Lecture Notes in Computer Science, vol 4076, pages 510-524, Springer, 2006.

Ulas, M., “Rational points on certain hyperelliptic curves over finite fields.”, Polish Academy of Sciences, 55(2): 97-104, 2007