Internet Engineering Task Force (IETF)
Request for Comments: 8110
Category: Informational
ISSN: 2070-1721

D. Harkins, Ed.
HP Enterprise
W. Kumari, Ed.
Google

March 2017

Opportunistic Wireless Encryption

Abstract

This memo specifies an extension to IEEE Std 802.11 to provide for opportunistic (unauthenticated) encryption to the wireless media.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8110.

Copyright Notice

Table of Contents

1. Introduction

This memo describes Opportunistic Wireless Encryption (OWE) -- a mode of opportunistic security [RFC7435] for IEEE Std 802.11 that provides encryption of the wireless medium but no authentication.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

1.2. Notation

This memo uses the following notation:

y = F(X)
: An element-to-scalar mapping function. For an elliptic curve group, it takes a point on the curve and returns the x-coordinate; for a finite field element, it is the identity function, just returning the element itself.

Z = DH(x,Y)
: For an elliptic curve, DH(x,Y) is the multiplication of point Y by the scalar value x, creating a point on the curve Z; for finite field cryptography, DH(x,Y) is an exponentiation of element Y to the power of x (implied modulo a field defining prime, p) resulting in an element Z.

a = len(b)
: Indicates the length in bits of the string b.

2. Background

Internet access has become an expected service at many locations -- for example, coffee shops, airports, and hotels. In many cases, this is offered over "Open" (unencrypted) wireless networks, because distributing a passphrase (or using other authentication solutions) is not convenient or realistic. Ideally, users would always use a VPN when using an untrusted network, but often they don’t. This leaves their traffic vulnerable to sniffing attacks, for example, from someone in the adjacent hotel room running Wireshark, pervasive monitors, etc.

In addition, many businesses (for example, coffee shops and bars) offer free Wi-Fi as an inducement to customers to enter and remain in the premises. Many customers will use the availability of free Wi-Fi as a deciding factor in which business to patronize. Since these businesses are not Internet service providers, they are often unwilling and/or unqualified to perform complex configuration on their network. In addition, customers are generally unwilling to do complicated provisioning on their devices just to obtain free Wi-Fi. This leads to a popular deployment technique -- a network protected using a shared and public Pre-Shared Key (PSK) that is printed on a sandwich board at the entrance, on a chalkboard on the wall, or on a menu. The PSK is used in a cryptographic handshake, defined in [IEEE802.11], called the "4-way handshake" to prove knowledge of the PSK and derive traffic encryption keys for bulk wireless data.

The belief is that this protects the wireless medium from passive sniffing and simple attacks. That belief is erroneous. Since the PSK is known by everyone, it is possible for a passive attacker to observe the 4-way handshake and compute the traffic encryption keys used by a client and access point (AP). If the attacker is too late to observe this exchange, he can issue a forged "deauthenticate" frame that will cause the client and/or AP to reset the 802.11 state machine and cause them to go through the 4-way handshake again, thereby allowing the passive attacker to determine the traffic keys.

With OWE, the client and AP perform a Diffie-Hellman key exchange during the access procedure and use the resulting pairwise secret with the 4-way handshake instead of using a shared and public PSK in the 4-way handshake.

OWE requires no special configuration or user interaction but provides a higher level of security than a common, shared, and public PSK. OWE not only provides more security to the end user, it is also easier to use both for the provider and the end user because there are no public keys to maintain, share, or manage.

3. 802.11 Network Access

Wi-Fi access points (APs) advertise their presence through frames called "beacons". These frames inform clients within earshot of the SSID (Service Set Identifier) the AP is advertising, the AP’s Media Access Control (MAC) address (known as its "BSSID" (Basic Service Set Identifier)), security policy governing access, the symmetric ciphers it uses for unicast and broadcast frames, QoS information, as well as support for other optional features of [IEEE802.11]. Wi-Fi clients can actively discover APs by issuing "probe requests", which are queries for APs that respond with "probe responses". A probe response carries essentially the same information as a beacon.

After an AP is discovered by a client, actively through probing or passively through beacons, the client initiates a two-step method to gain network access. The first step is "802.11 authentication". For most methods of access, this is an empty exchange known as "Open Authentication" -- basically, the client says, "authenticate me", and the AP responds, "ok, you’re authenticated". After 802.11 authentication is 802.11 association, in which the client requests network access from an AP (the SSID, a selection of the type of subsequent authentication to be made, any pairwise and group ciphers, etc.) using an 802.11 association request. The AP acknowledges the request with an 802.11 association response.

If the network is Open (no authentication and no encryption), the client has network access immediately after completion of 802.11 association. If the network enforces PSK authentication, the 4-way handshake is initiated by the AP using the PSK to authenticate the client and derive traffic encryption keys.

To add an opportunistic encryption mode of access to [IEEE802.11], it is necessary to perform a Diffie-Hellman key exchange during 802.11 authentication and use the resulting pairwise secret with the 4-way handshake.

4. Opportunistic Wireless Encryption

4.1. Cryptography

Performing a Diffie-Hellman key exchange requires agreement on a domain parameter set in which to perform the exchange. OWE uses a registry (see [IKE-IANA]) to map an integer into a complete domain parameter set. OWE supports both Elliptic Curve Cryptography (ECC) and Finite Field Cryptography (FFC).

OWE uses a hash algorithm for generation of a secret and a secret identifier. The particular hash algorithm depends on the group chosen for the Diffie-Hellman. For ECC, the hash algorithm depends on the size of the prime defining the curve p:

- SHA-256: when len(p) <= 256

- SHA-384: when 256 < len(p) <= 384

- SHA-512: when 384 < len(p)

For FFC, the hash algorithm depends on the prime, p, defining the finite field:

- SHA-256: when len(p) <= 2048

- SHA-384: when 2048 < len(p) <= 3072

- SHA-512: when 3072 < len(p)

4.2. OWE Discovery

An access point advertises support for OWE using an Authentication and Key Management (AKM) suite selector for OWE. This AKM is illustrated in Table 1 and is added to the Robust Security Network (RSN) element, defined in [IEEE802.11], in all beacons and probe response frames the AP issues.

OUI	Suite Type	Authentication Type	Key Management Type	Key derivation type
00-0F-AC	18	Opportunistic Wireless Encryption	This document	[RFC5869]

Table 1: OWE AKM

Once a client discovers an OWE-compliant AP, it performs "Open System" 802.11 authentication as defined in [IEEE802.11], and it then proceeds to 802.11 association.

4.3. OWE Association

Information is added to 802.11 association requests and responses using TLVs that [IEEE802.11] calls "elements". Each element has an "Element ID" (including any Element ID extension), a length, and a value field that is element specific. These elements are appended to each other to construct 802.11 association requests and responses.

OWE adds the Diffie-Hellman Parameter element (see Figure 1) to 802.11 association requests and responses. The client adds her public key in the 802.11 association request, and the AP adds his public key in the 802.11 association response.

```
+------------+----------+-----------+-----------------------+
| Element ID |  Length  | Element ID |   element-specific    |
|            |          |  Extension |         data          |
+------------+----------+-----------+---------+-------------+
|    255     | variable |     32    | group   |  public key |
+------------+----------+-----------+---------+-------------+
```

Figure 1: The Diffie-Hellman Parameter Element

where:

- o group is an unsigned two-octet integer defined in [IKE-IANA], in little-endian format, that identifies a domain parameter set;

- o public key is an octet string representing the Diffie-Hellman public key; and,

- o Element ID, Length, and Element ID Extension are all single-octet integers.

The encoding of the public key depends on its type. FFC elements SHALL be encoded per the integer-to-octet-string conversion technique of [RFC6090]. For ECC elements, the encoding depends on the definition of the curve, either that in [RFC6090] or [RFC7748]. If the public key is from a curve defined in [RFC6090], compact representation SHALL be used.

A client wishing to do OWE MUST indicate the OWE AKM in the RSN element portion of the 802.11 association request and MUST include a Diffie-Hellman Parameter element to its 802.11 association request. An AP agreeing to do OWE MUST include the OWE AKM in the RSN element portion of the 802.11 association response. If "PMK caching" (see Section 4.5) is not performed, it MUST also include a Diffie-Hellman Parameter element. If "PMK caching" is not being performed, a client MUST discard any 802.11 association response that indicates the OWE

AKM in the RSN element but does not have not a Diffie-Hellman Parameter element.

For interoperability purposes, a compliant implementation MUST support group nineteen (19), a 256-bit elliptic curve group. If the AP does not support the group indicated in the received 802.11 association request, it MUST respond with an 802.11 association response with a status code of seventy-seven (77) indicating an unsupported finite cyclic group. A client that receives an 802.11 association response with a status code of seventy-seven SHOULD retry OWE with a different supported group and, due to the unsecured nature of 802.11 association, MAY request association again using the group that resulted in failure. This failure SHOULD be logged, and if the client abandons association due to the failure to agree on any group, notification of this fact SHOULD be provided to the user.

Received Diffie-Hellman Parameter elements are checked for validity upon receipt. For ECC, a validity check depends on the curve definition, either that in [RFC6090] or [RFC7748]. For FFC, elements are checked that they are between one (1) and one (1) less than the prime, p, exclusive (i.e., 1 < element < p-1). Invalid received Diffie-Hellman keys MUST result in unsuccessful association, a failure of OWE, and a reset of the 802.11 state machine. Due to the unsecured nature of 802.11 association, a client SHOULD retry OWE a number of times (this memo does not specify the number of times). This failure should be logged, and if the client abandons association due to the (repeated) receipt of invalid elements, notification of this fact should be provided to the user.

4.4. OWE Post-Association

Once the client and AP have finished 802.11 association, they then complete the Diffie-Hellman key exchange and create a Pairwise Master Key (PMK) and its associated identifier, PMKID [IEEE802.11]. Given a private key x and the peer’s (AP’s if client, client’s if AP) public key Y, the following are generated:

```
   z = F(DH(x, Y))

   prk = HKDF-extract(C | A | group, z)

   PMK = HKDF-expand(prk, "OWE Key Generation", n)
```

where HKDF-expand() and HKDF-extract() are defined in [RFC5869]; "C | A | group" is a concatenation of the client’s Diffie-Hellman public key, the AP’s Diffie-Hellman public key (from the 802.11 association request and response, respectively), and the two-octet group from the Diffie-Hellman Parameter element (in little-endian format) and is passed as the salt to the HMAC-based Extract-and-Expand Key Derivation Function (HKDF) using the hash algorithm defined in Section 4.1; and n is the bit length of the digest produced by that hash algorithm. z and prk SHOULD be irretrievably deleted once the PMK has been generated.

The PMKID is generated by hashing the two Diffie-Hellman public keys (the data, as sent and received, from the "public key" portion of the Diffie-Hellman Parameter element in the 802.11 association request and response) and returning the leftmost 128 bits:

```
   PMKID = Truncate-128(Hash(C | A))
```

where C is the client’s Diffie-Hellman public key from the 802.11 association request, A is the AP’s Diffie-Hellman public key from the 802.11 association response, and Hash is the hash algorithm defined in Section 4.1.

Hash	Integrity Algorithm	KCK_bits	Size of MIC	Key-wrap Algorithm	KEK_bits
SHA-256	HMAC-SHA-256	128	16	NIST AES Key-wrap	128
SHA-384	HMAC-SHA-384	192	24	NIST AES Key-wrap	256
SHA-512	HMAC-SHA-521	256	32	NIST AES Key-wrap	256

Table 2: Integrity and Key Wrap Algorithms

Upon completion of 802.11 association, the AP initiates the 4-way handshake to the client using the PMK generated above. The 4-way handshake generates a Key-Encrypting Key (KEK), a Key-Confirmation Key (KCK), and a Message Integrity Code (MIC) to use for protection of the frames that define the 4-way handshake. The algorithms and key lengths used in the 4-way handshake depend on the hash algorithm selected in Section 4.1 and are listed in Table 2.

The result of the 4-way handshake is encryption keys to protect bulk unicast data and broadcast data. If the 4-way handshake fails, this information SHOULD be presented to the user.

4.5. OWE PMK Caching

[IEEE802.11] defines "PMK caching" where a client and access point can cache a PMK for a certain period of time and reuse it with the 4-way handshake after subsequent associations to bypass potentially expensive authentication. A client indicates its desire to do "PMK caching" by including the identifying PMKID in its 802.11 association request. If an AP has cached the PMK identified by that PMKID, it includes the PMKID in its 802.11 association response; otherwise, it ignores the PMKID and proceeds with normal 802.11 association. OWE supports the notion of "PMK caching".

Since "PMK caching" is indicated in the same frame as the Diffie-Hellman Parameter element is passed, a client wishing to do "PMK caching" MUST include both in her 802.11 association request. If the AP has the PMK identified by the PMKID and wishes to perform "PMK caching", he will include the PMKID in his 802.11 association response but does not include a Diffie-Hellman Parameter element. If the AP does not have the PMK identified by the PMKID, it ignores the PMKID and proceeds with normal OWE 802.11 association by including a Diffie-Hellman Parameter element.

When attempting "PMK caching", a client SHALL ignore any Diffie-Hellman Parameter element in an 802.11 association response whose PMKID matches that of the client-issued 802.11 association request. If the 802.11 association response does not include a PMKID, or if the PMKID does not match that of the client-issued 802.11 association request, the client SHALL proceed with normal OWE association.

The client SHALL ignore a PMKID in any 802.11 association response frame for which it did not include a PMKID in the corresponding 802.11 association request frame.

5. IANA Considerations

This document does not require any IANA actions.

6. Implementation Considerations

OWE is a replacement for 802.11 "Open" authentication. Therefore, when OWE-compliant access points are discovered, the presentation of the available SSID to users should not include special security symbols such as a "lock icon". To a user, an OWE SSID is the same as "Open"; it simply provides more security behind the scenes.

When OWE is initially deployed as a replacement for an existing network that uses "Open" authentication or a shared and public PSK, it will be necessary to create an additional Basic Service Set

Identifier (BSSID) or a new Extended Service Set (ESS) with a separate Service Set Identifier (SSID) for OWE so two distinct 802.11 networks can exist on the same access point (see [IEEE802.11]). This arrangement should remain until the majority of users have switched over to OWE.

7. Security Considerations

Opportunistic encryption does not provide authentication. The client will have no authenticated identity for the access point, and vice versa. They will share pairwise traffic encryption keys and have a cryptographic assurance that a frame claimed to be from the peer is actually from the peer and was not modified in flight.

OWE only secures data sent over the wireless medium and does not provide security for end-to-end traffic. Users should still use application-level security to achieve security end-to-end.

OWE is susceptible to an active attack in which an adversary impersonates an access point and induces a client to connect to it via OWE while it makes a connection to the legitimate access point. In this particular attack, the adversary is able to inspect, modify, and forge any data between the client and legitimate access point.

OWE is not a replacement for any authentication protocol specified in [IEEE802.11] and is not intended to be used when an alternative that provides real authentication is available.

8. References

8.1. Normative References

[IEEE802.11]
IEEE, "IEEE Standard for Information technology-- Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11, DOI 10.1109/IEEESTD.2016.7786995.

[IKE-IANA] IANA, "Transform Type 4 - Diffie-Hellman Group Transform IDs", <http://www.iana.org/assignments/ikev2-parameters/>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <http://www.rfc-editor.org/info/rfc5869>.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, DOI 10.17487/RFC6090, February 2011, <http://www.rfc-editor.org/info/rfc6090>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <http://www.rfc-editor.org/info/rfc7748>.

8.2. Informative References

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <http://www.rfc-editor.org/info/rfc7435>.

Authors’ Addresses

Dan Harkins (editor)
HP Enterprise
3333 Scott Boulevard
Santa Clara, California 95054
United States of America

Phone: +1 415 555 1212
Email: dharkins@arubanetworks.com

Warren Kumari (editor)
Google
1600 Amphitheatre Parkway
Mountain View, California 94043
United States of America

Phone: +1 408 555 1212
Email: warren@kumari.net