capport
Internet-Draft
Intended status: Informational
Expires: January 19, 2017

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

July 18, 2016

OWE
draft-harkins-owe-00

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 Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 19, 2017.

Table of Contents

1. Introduction

This memo describes a mode of opportunistic encryption [RFC7435] for 802.11 -- OWE -- 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 expontiation 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

Many businesses-- bars, coffee shops, etc.-- 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 not willing and/or not qualified 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 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. If the attacker is too late to observe this exchange, he can issue a forged "de-authenticate" 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.

Basically, this shared and public PSK mode of access is as bad as an open and unencrypted network. [TODO: Explain trade offs; shared PSK means the attacker has to be active and could provide a false sense of security.] With OWE, the client and AP, would 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 provides more security to the end user, while also being easier to use (no public keys to maintain, share, etc.).

3. 802.11 Network Access

Wi-Fi Access Points advertise their presence through frames called "beacons". These frames inform clients within earshot of the SSID the AP is advertising, the AP's MAC address (known as its "BSSID"),

security policy governing access, which 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 (SAE being the exception), this is an empty exchange known as "Open Authentication-- basically the client says, "authenticate me", and the AP resonds "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, 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 identifer for OWE. This AKM is illustrated in Table 1 and is added to the RSN Element in all beacons and probe responses that the AP issues.

OWE AKM

OUI	Suite Type	Authentication Type	Key Manamgement Type	Key derivation type
00-0F-AC	ANA-1	Opportunistic Wireless Encryption	This document	[RFC5869]

Table 1: OWE AKM

where ANA-1 is assigned by IEEE 802.11 ANA.

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

4.3. OWE Association

Information is added to 802.11 association requests and responses by 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 associate 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 associate request and the AP adds his public key in the 802.11 associate response.

The Diffie-Hellman Parameter Element

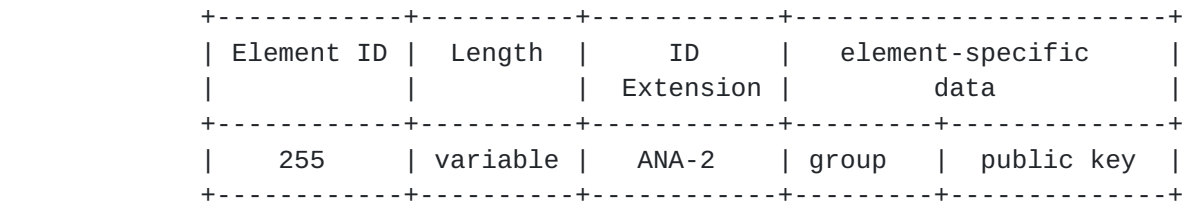

Figure 1

where

- ANA-2 is assigned by IEEE 802.11 ANA;
- group is an unsigned two-octet integer defined in [IKE-IANA], in little-endian format, that identifies a domain parameter set;
- public key is an octet string representing the Diffie-Hellman public key encoded according to section 2.3.3 (Elliptic Curve to Octet String Conversion) or 2.3.5 (Field Element to Octet String Conversion) of [SEC1] depending on whether the public key is ECC or FFC, respectively; and,
- Element ID, Length, and ID Extension are all single octet integers in little-endian format.

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. TODO: what to do if the AP doesn't like the client's chosen group?

Received Diffie-Hellman Parameter Elements are checked for validity upon receipt. For ECC, elements are checked by verifying that equation for the curve is correct for the given x- and y-

coordinates, excluding the point at infinity. 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 and a failure of OWE.

4.4. OWE Post-Association

Once the client and AP have finished 802.11 association they finish the Diffie-Hellman key exchange and create a "pairwise master key" (PMK), and its associated identifier, PMKID. 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(NULL, z)

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

Where HKDF-expand() and HKDF-extract() are defined in [RFC5869], NULL indicates the "salt-less" invocation of HKDF using the hash algorithm defined in section Section 4.1, and n is the bitlength of the digest produced by that hash algorithm. z and prk are 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 left-most 128 bits:

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

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

Upon completion of 802.11 association, the AP initiates the 4-way Handshake to the client using the PMK generated above. The result of the 4-way Handshake are encryption keys to protect bulk unicast data and broadcast data.

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 Parameeter element.

When attempting "PMK caching" a client SHALL ignore any Diffie-Hellman Parameter element in an 802.11 association response that 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 memo includes no request to IANA.

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 does not include special security symbols such as a graphic lock. To a user, an OWE SSID is the same as "Open", it just provides more security behind the scenes.

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 is susceptible to an active attack in which an adversary impersonates an Access Point, 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. Normative References

[IEEE802.11] IEEE Computer Society, "Telecommunications and information exchange between systems Local and metropolitan area networks--", Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications IEEE Std 802.11-2012, 2012.

[IKE-IANA] IANA, "Internet Key Exchange (version 2) Parameters", Transform Type 4: Diffie-Hellman Group Transform IDs, 2005, <http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-8>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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>.

[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>.

[SEC1] Brown, D., "Elliptic Curve Cryptography", Version 2.0, 2009.

Authors' Addresses

Dan Harkins (editor)
HP Enterprise
1322 Crossman avenue
Sunnyvale, California 94089
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