Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 19, 2017

J. Mattsson
D. Migault
Ericsson

May 18, 2017

ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for Transport Layer Security (TLS)
draft-ietf-tls-ecdhe-psk-aead-04

Abstract

This document defines several new cipher suites for the Transport Layer Security (TLS) protocol. The cipher suites are all based on the Ephemeral Elliptic Curve Diffie-Hellman with Pre-Shared Key (ECDHE_PSK) key exchange together with the Authenticated Encryption with Associated Data (AEAD) algorithms AES-GCM and AES-CCM. PSK provides light and efficient authentication, ECDHE provides forward secrecy, and AES-GCM and AES-CCM provides encryption and integrity protection.

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 November 19, 2017.

Copyright Notice

Table of Contents

1. Requirements notation

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 [RFC2119].

2. Introduction

This document defines new cipher suites that provide Pre-Shared Key (PSK) authentication, Perfect Forward Secrecy (PFS), and Authenticated Encryption with Associated Data (AEAD). The cipher suites are defined for version 1.2 of the Transport Layer Security (TLS) [RFC5246] protocol, version 1.2 of the Datagram Transport Layer Security (DTLS) protocol [RFC6347], as well as version 1.3 of TLS [I-D.ietf-tls-tls13].

Pre-Shared Key (PSK) Authentication is widely used in many scenarios. One deployment is 3GPP networks where pre-shared keys are used to authenticate both subscriber and network. Another deployment is Internet of Things where PSK authentication is often preferred for performance and energy efficiency reasons. In both scenarios the endpoints are owned/controlled by a party that provisions the pre-shared keys and makes sure that they provide a high level of entropy.

Perfect Forward Secrecy (PFS) is a strongly recommended feature in security protocol design and can be accomplished by using an ephemeral Diffie-Hellman key exchange method. Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) provides PFS with excellent performance

and small key sizes. ECDHE is mandatory to implement in both HTTP/2 [RFC7540] and CoAP [RFC7252].

AEAD algorithms that combine encryption and integrity protection are strongly recommended for (D)TLS [RFC7525] and non-AEAD algorithms are forbidden to use in TLS 1.3 [I-D.ietf-tls-tls13]. The AEAD algorithms considered in this document are AES-GCM and AES-CCM. The use of AES-GCM in TLS is defined in [RFC5288] and the use of AES-CCM is defined in [RFC6655].

[RFC4279] defines Pre-Shared Key (PSK) cipher suites for TLS but does not consider Elliptic Curve Cryptography. [RFC4492] introduces Elliptic Curve Cryptography for TLS but does not consider PSK authentication. [RFC5487] describes the use of AES-GCM in combination with PSK authentication, but does not consider ECDHE. [RFC5489] describes the use of PSK in combination with ECDHE but does not consider AES-GCM or AES-CCM.

3. ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites

The cipher suites defined in this document are based on the AES-GCM and AES-CCM Authenticated Encryption with Associated Data (AEAD) algorithms AEAD_AES_128_GCM, AEAD_AES_256_GCM and AEAD_AES_128_CCM defined in [RFC5116], and AEAD_AES_128_CCM_8 defined in [RFC6655].

Messages and pre-master secret construction in this document are defined in [RFC5489]. The ServerKeyExchange and ClientKeyExchange messages are used and the pre-master secret is computed as for the ECDHE_PSK key exchange. The elliptic curve parameters used in in the Diffie-Hellman parameters are negotiated using extensions defined in [I-D.ietf-tls-rfc4492bis].

For TLS 1.2, the following cipher suites are defined:

```
TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256   = {0xTBD,0xTBD};
TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384   = {0xTBD,0xTBD};
```

```
TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256 = {0xTBD,0xTBD};
TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256   = {0xTBD,0xTBD};
```

The assigned code points can only be used for TLS 1.2.

4. Applicable TLS Versions

The cipher suites defined in this document MUST NOT be negotiated for any version of (D)TLS other than TLS 1.2.

TLS version 1.3 and later negotiate these features in a different manner. Unlike TLS 1.2, TLS 1.3 separates authentication and cipher

suite negotiation [I-D.ietf-tls-tls13] Section 1.2. TLS 1.3 supports PSK with ECDHE key exchange and the cipher suites TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_AES_128_CCM_8_SHA256 and TLS_AES_128_CCM_SHA256 are part of the specification. As a result, TLS 1.3 and higher versions, negotiate and support these cipher suites in a different way.

The cipher suites defined in this document make use of the authenticated encryption with additional data (AEAD) defined in TLS 1.2 [RFC5246] and DTLS 1.2 [RFC6347]. Earlier versions of TLS do not have support for AEAD and consequently, the cipher suites defined in this document MUST NOT be negotiated in TLS versions prior to 1.2. In addition, it is worth noting that TLS 1.0 [RFC2246] and TL1.2 [RFC4346] splits the pre-master in two parts. The PRF results from mixing the two pseudorandom streams with distinct hash functions (MD5 and SHA-1) by exclusive-ORing them together. In the case of ECDHE_PSK authentication, the PSK and pre-master are treated by distinct hash function with distinct properties. This may introduce vulnerabilities over the expected security provided by the constructed pre-master. As such TLS 1.0 and TLS 1.1 should not be used with ECDHE_PSK.

A client that offers the cipher suites from this document in ClientHello.cipher_suites in combination with (3,1) "TLS 1.0" or (3,2) "TLS 1.1" in ClientHello.client_version MUST support TLS 1.2 and MUST accept the server to negotiate TLS 1.2 for the current session. If the client does not support TLS 1.2 or is not willing to negotiate TLS 1.2, then this client MUST NOT offer any of these cipher suites with a lower protocol version than (3,3) "TLS 1.2" in

ClientHello.client_version.

A server receiving a ClientHello and a client_version indicating (3,1) "TLS 1.0" or (3,2) "TLS 1.1" and any of the cipher suites from this document in ClientHello.cipher_suites can safely assume that the client supports TLS 1.2 and is willing to use it. The server MUST NOT negotiate these cipher suites with TLS protocol versions earlier than TLS 1.2. Not requiring clients to indicate their support for TLS 1.2 cipher suites exclusively through ClientHello.client_hello improves the interoperability in the installed base and use of TLS 1.2 AEAD cipher suites without upsetting the installed base of version-intolerant TLS servers, results in more TLS handshakes succeeding and obviates fallback mechanisms.

5. IANA Considerations

This document defines the following new cipher suites, whose values have been assigned in the TLS Cipher Suite Registry defined by [RFC5246].


```
TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256   = {0xTBD; 0xTBD} {0xD0,0x01};
TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384   = {0xTBD; 0xTBD} {0xD0,0x02};
TLS_ECDHE_PSK_WITH_AES_128_CCM_8_SHA256 = {0xTBD; 0xTBD} {0xD0,0x03};
TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256   = {0xTBD; 0xTBD} {0xD0,0x05};
```

NOTE TO THE RFC EDITOR: PLEASE REMOVE THIS PARAGRAPH. The cipher suite numbers listed in the last column are numbers used for cipher suite interoperability testing and it's suggested that IANA use these values for assignment.

6. Security Considerations

The security considerations in TLS 1.2 [RFC5246], DTLS 1.2 [RFC6347], TLS 1.3 [I-D.ietf-tls-tls13], ECDHE_PSK [RFC5489], AES-GCM [RFC5288], and AES-CCM [RFC6655] apply to this document as well.

All the cipher suites defined in this document provide confidentiality, mutual authentication, and forward secrecy. The AES-128 cipher suites provide 128-bit security and the AES-256 cipher suites provide at least 192-bit security. However, AES_128_CCM_8 only provides 64-bit security against message forgery.

Use of Pre-Shared Keys of limited entropy may allow an active attacker attempts to connect to the server and try different keys. For example, limited entropy may be provided by using a short PSK in which case an attacker may perform a brute-force attack. Another example includes the use of a PSK chosen by a human which thus may be exposed to dictionary attacks.

The Pre-Shared Keys used for authentication MUST have a security level equal or higher than the cipher suite used, i.e., at least 128-bit for the AES-128 cipher suites and at least 192-bit for the AES-256 cipher suites.

GCM or CCM encryption - even of different clear text - re-using a nonce with a same key undermines the security of GCM and CCM. As a result, GCM and CCM MUST only be used with a system guaranteeing nonce uniqueness [RFC5116].

7. Acknowledgements

The authors would like to thank Ilari Liusvaara, Eric Rescorla, Dan Harkins, Russ Housley, Dan Harkins, Martin Thomson, Nikos Mavrogiannopoulos, Peter Dettman, Xiaoyin Liu, Joseph Salowey, Sean Turner Dave Garrett, Martin Rex and Kathleen Moriarty for their valuable comments and feedback.

8. References

8.1. Normative References

[I-D.ietf-tls-rfc4492bis]
Nir, Y., Josefsson, S., and M. Pegourie-Gonnard, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier", draft-ietf-tls-rfc4492bis-17 (work in progress), May 2017.

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-20 (work in progress), April 2017.

[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>.

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, DOI 10.17487/RFC2246, January 1999, <http://www.rfc-editor.org/info/rfc2246>.

[RFC4279] Eronen, P., Ed. and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, DOI 10.17487/RFC4279, December 2005, <http://www.rfc-editor.org/info/rfc4279>.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, DOI 10.17487/RFC4346, April 2006, <http://www.rfc-editor.org/info/rfc4346>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <http://www.rfc-editor.org/info/rfc5116>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, DOI 10.17487/RFC5288, August 2008, <http://www.rfc-editor.org/info/rfc5288>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <http://www.rfc-editor.org/info/rfc6347>.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, DOI 10.17487/RFC6655, July 2012, <http://www.rfc-editor.org/info/rfc6655>.

8.2. Informative References

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, DOI 10.17487/RFC4492, May 2006, <http://www.rfc-editor.org/info/rfc4492>.

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, DOI 10.17487/RFC5487, March 2009, <http://www.rfc-editor.org/info/rfc5487>.

[RFC5489] Badra, M. and I. Hajjeh, "ECDHE_PSK Cipher Suites for Transport Layer Security (TLS)", RFC 5489, DOI 10.17487/RFC5489, March 2009, <http://www.rfc-editor.org/info/rfc5489>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <http://www.rfc-editor.org/info/rfc7252>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <http://www.rfc-editor.org/info/rfc7525>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <http://www.rfc-editor.org/info/rfc7540>.

Authors' Addresses

John Mattsson

Ericsson AB
SE-164 80 Stockholm
Sweden

Phone: +46 76 115 35 01
Email: john.mattsson@ericsson.com

Daniel Migault
Ericsson
8400 boulevard Decarie
Montreal, QC   H4P 2N2
Canada

Phone: +1 514-452-2160
Email: daniel.migault@ericsson.com