Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 20, 2016

J. Mattsson
D. Migault
Ericsson

April 18, 2016

ECDHE_PSK with AES-GCM and AES-CCM Cipher Suites for Transport Layer Security (TLS)
draft-mattsson-tls-ecdhe-psk-aead-05

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 perfect forward secrecy, and AES-GCM and AES-CCM provides encryption and integrity protection.

Status of This Memo

Copyright Notice

Table of Contents

1. 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 or later of the the Transport Layer Security (TLS) [RFC5246] protocol, as well as version 1.2 or later of the Datagram Transport Layer Security (DTLS) protocol [RFC6347].

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 [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.

2. 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, AEAD_AES_128_CCM, and AEAD_AES_256_CCM defined in [RFC5116], AEAD_AES_128_CCM_8 and AEAD_AES_256_CCM_8 defined in [RFC6655]. 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_256_CCM_8_SHA256 = {0xTBD,0xTBD};
TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256   = {0xTBD,0xTBD};
TLS_ECDHE_PSK_WITH_AES_256_CCM_SHA384   = {0xTBD,0xTBD};
```

For the AES-128 cipher suites, the TLS Pseudorandom Function (PRF) with SHA-256 as the hash function SHALL be used and Clients and Servers MUST NOT negotiate curves of less than 255 bits.

For the AES-256 cipher suites, the TLS PRF with SHA-384 as the hash function SHALL be used and Clients and Servers MUST NOT negotiate curves of less than 384 bits.

When used in TLS 1.2, the keying material is derived as described in [RFC5489] and [RFC5246] and nonces are constructed as described in [RFC5288], and [RFC6655]. When used in TLS 1.3, the keying material is derived as described in [I-D.ietf-tls-tls13], and the nonces are constructed as described in [I-D.ietf-tls-tls13].

3. Applicable TLS Versions

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, these cipher suites MUST NOT be negotiated in TLS versions prior to 1.2. Clients MUST NOT offer

these cipher suites if they do not offer TLS 1.2 or later. Servers, which select an earlier version of TLS MUST NOT select one of these cipher suites. A client MUST treat the selection of these cipher suites in combination with a version of TLS that does not support AEAD (i.e., TLS 1.1 or earlier) as an error and generate a fatal 'illegal_parameter' TLS alert.

4. 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_256_CCM_8_SHA256 = {0xTBD; 0xTBD} {0xD0,0x04};
TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256   = {0xTBD; 0xTBD} {0xD0,0x05};
TLS_ECDHE_PSK_WITH_AES_256_CCM_SHA384   = {0xTBD; 0xTBD} {0xD0,0x06};
```

The cipher suite numbers listed in the second column are numbers used for cipher suite interoperability testing and it's suggested that IANA use these values for assignment.

5. 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 perfect 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 and AES_256_GCM and AES_256_CCM only provide 128-bit security against message forgery.

Use of Pre-Shared Keys of limited entropy (for example, a PSK that is relatively short, or was chosen by a human and thus may contain less entropy than its length would imply) may allow an active attacker to perform a brute-force attack where the attacker attempts to connect to the server and tries different keys. Passive eavesdropping alone is not sufficient. For these reasons 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.

6. Acknowledgements

The authors would like to thank Ilari Liusvaara, Eric Rescorla, Dan Harkins, Russ Housley and Sean Turner for their valuable comments and feedback.

7. References

7.1. Normative References

[I-D.ietf-tls-tls13]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", draft-ietf-tls-tls13-12 (work in progress), March 2016.

[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>.

[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>.

[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>.

[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>.

[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>.

7.2. Informative References

[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>.

[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