TLS Working Group   Mohamad Badra
Internet Draft   LIMOS Laboratory
Intended status: Standards Track   September 25, 2008
Expires: March 2009

**Pre-Shared Key Cipher Suites for Transport Layer Security (TLS) with
SHA-256/384 and AES Galois Counter Mode
draft-ietf-tls-psk-new-mac-aes-gcm-03.txt**

Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF), its areas, and its working groups. Note that
   other groups may also distribute working documents as Internet-
   Drafts.

   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."

   The list of current Internet-Drafts can be accessed at
   http://www.ietf.org/ietf/1id-abstracts.txt

   The list of Internet-Draft Shadow Directories can be accessed at
   http://www.ietf.org/shadow.html

   This Internet-Draft will expire on March 25, 2009.

Copyright Notice

Abstract

   RFC 4279 and RFC 4785 describe pre-shared key cipher suites for
   Transport Layer Security (TLS). However, all those cipher suites
   use SHA-1 as their MAC algorithm. This document describes a set of
   pre-shared key cipher suites for TLS which uses stronger digest
   algorithms (i.e., SHA-256 or SHA-384) and another set which uses the
   Advanced Encryption Standard (AES) in Galois Counter Mode (GCM).

Table of Contents

1. Introduction

The benefits of pre-shared symmetric-key vs. public-/private-key pair based authentication for the key exchange in TLS have been explained in the Introduction of [RFC4279]. This document leverages the already defined algorithms for the application of newer, generally regarded stronger, cryptographic primitives and building blocks.

TLS 1.2 [RFC5246] adds support for authenticated encryption with additional data (AEAD) cipher modes [RFC5116]. This document describes the use of Advanced Encryption Standard (AES) [AES] in Galois Counter Mode (GCM) [GCM] (AES-GCM) with various pre-shared key (PSK) authenticated key exchange mechanisms ([RFC4279] and [RFC4785]) in cipher suites for Transport Layer Security (TLS).

This document also specifies PSK cipher suites for TLS which replace SHA-1 by SHA-256 or SHA-384 [SHS]. RFC 4279 [RFC4279] and RFC 4785 [RFC4785] describe PSK cipher suites for TLS. However, all of the RFC 4279 and the RFC 4785 cipher suites use HMAC-SHA1 as their MAC algorithm. Due to recent analytic work on SHA-1 [Wang05], the IETF is gradually moving away from SHA-1 and towards stronger hash algorithms.

Related TLS cipher suites with key exchange algorithms that are authenticated using public/private key pairs have recently been specified:

   - RSA, DSS, and Diffie-Hellman based cipher suites in [RFC5288], and

   -ECC based cipher suites with SHA-256/384 and AES-GCM in [RFC5289].

The reader is expected to become familiar with these two memos prior to studying this document.

1.1. Conventions used in this document

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. PSK, DHE_PSK and RSA_PSK Key Exchange Algorithms with AES-GCM

The following six cipher suites use the new authenticated encryption modes defined in TLS 1.2 with AES in Galois Counter Mode (GCM)

[GCM]. The cipher suites with DHE_PSK key exchange algorithm
(TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 and
TLS_DHE_PSK_WITH_AES_256_GCM_SHA348) provide Perfect Forward Secrecy
(PFS).

```
   CipherSuite TLS_PSK_WITH_AES_128_GCM_SHA256        = {0xXX,0xXX};
   CipherSuite TLS_PSK_WITH_AES_256_GCM_SHA384        = {0xXX,0xXX};
   CipherSuite TLS_DHE_PSK_WITH_AES_128_GCM_SHA256    = {0xXX,0xXX};
   CipherSuite TLS_DHE_PSK_WITH_AES_256_GCM_SHA384    = {0xXX,0xXX};
   CipherSuite TLS_RSA_PSK_WITH_AES_128_GCM_SHA256    = {0xXX,0xXX};
   CipherSuite TLS_RSA_PSK_WITH_AES_256_GCM_SHA384    = {0xXX,0xXX};
```

These cipher suites use authenticated encryption with additional
data (AEAD) algorithms AEAD_AES_128_GCM and AEAD_AES_256_GCM as
described in RFC 5116. GCM is used as described in [RFC5288].

The PSK, DHE_PSK and RSA_PSK key exchanges are performed as defined
in [RFC4279].

The PRFs SHALL be as follows:

   For cipher suites ending with _SHA256, the PRF is the TLS PRF
   [RFC5246] with SHA-256 as the hash function.

   For cipher suites ending with _SHA384, the PRF is the TLS PRF
   [RFC5246] with SHA-384 as the hash function.

Implementations MUST send a TLS Alert 'bad_record_mac' for all types
of failures encountered in processing the AES-GCM algorithm.

3. PSK, DHE_PSK and RSA_PSK Key Exchange with SHA-256/384

The cipher suites described in this section use AES [AES] in CBC
[CBC] mode with an HMAC-based MAC.

3.1. PSK Key Exchange Algorithm with SHA-256/384

```
   CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA256        = {0xXX,0xXX};
   CipherSuite TLS_PSK_WITH_AES_256_CBC_SHA384        = {0xXX,0xXX};
   CipherSuite TLS_PSK_WITH_NULL_SHA256               = {0xXX,0xXX};
   CipherSuite TLS_PSK_WITH_NULL_SHA384               = {0xXX,0xXX};
```

The above four cipher suites are the same as the corresponding
cipher suites in RFC 4279 and RFC 4785 (with names ending in "_SHA"
in place of "_SHA256" or "_SHA384"), except for the hash and PRF
algorithms.

The PRF and MAC algorithms SHALL be as follows:

> For cipher suites ending with _SHA256, the PRF is the TLS PRF
> [RFC5246] with SHA-256 as the hash function.
> The MAC is HMAC [RFC2104] with SHA-256 as the hash function.

> For cipher suites ending with _SHA384, the PRF is the TLS PRF
> [RFC5246] with SHA-384 as the hash function.
> The MAC is HMAC [RFC2104] with SHA-384 as the hash function.

3.2. DHE_PSK Key Exchange Algorithm with SHA-256/384

```
CipherSuite TLS_DHE_PSK_WITH_AES_128_CBC_SHA256    = {0xXX,0xXX};
CipherSuite TLS_DHE_PSK_WITH_AES_256_CBC_SHA384    = {0xXX,0xXX};
CipherSuite TLS_DHE_PSK_WITH_NULL_SHA256           = {0xXX,0xXX};
CipherSuite TLS_DHE_PSK_WITH_NULL_SHA384           = {0xXX,0xXX};
```

The above four cipher suites are the same as the corresponding
cipher suites in RFC 4279 and RFC 4785 (with names ending in "_SHA"
in place of "_SHA256" or "_SHA384"), except for the hash and PRF
algorithms, as explained in section 3.1.

3.3. RSA_PSK Key Exchange Algorithm with SHA-256/384

```
CipherSuite TLS_RSA_PSK_WITH_AES_128_CBC_SHA256    = {0xXX,0xXX};
CipherSuite TLS_RSA_PSK_WITH_AES_256_CBC_SHA384    = {0xXX,0xXX};
CipherSuite TLS_RSA_PSK_WITH_NULL_SHA256           = {0xXX,0xXX};
CipherSuite TLS_RSA_PSK_WITH_NULL_SHA384           = {0xXX,0xXX};
```

The above four cipher suites are the same as the corresponding
cipher suites in RFC 4279 and RFC 4785 (with names ending in "_SHA"
in place of "_SHA256" or "_SHA384"), except for the hash and PRF
algorithms, as explained in section 3.1.

4. Security Considerations

The security considerations in [RFC4279], [RFC4758] and [RFC5288]
apply to this document as well. In addition, as described in
[RFC5288], these cipher suites may only be used with TLS 1.2 or
greater.

5. IANA Considerations

IANA has assigned the following values for the cipher suites defined
in this document:

```
    CipherSuite TLS_PSK_WITH_AES_128_GCM_SHA256        = {0xXX,0xXX};
    CipherSuite TLS_PSK_WITH_AES_256_GCM_SHA384        = {0xXX,0xXX};
    CipherSuite TLS_DHE_PSK_WITH_AES_128_GCM_SHA256    = {0xXX,0xXX};
    CipherSuite TLS_DHE_PSK_WITH_AES_256_GCM_SHA384    = {0xXX,0xXX};
    CipherSuite TLS_RSA_PSK_WITH_AES_128_GCM_SHA256    = {0xXX,0xXX};
    CipherSuite TLS_RSA_PSK_WITH_AES_256_GCM_SHA384    = {0xXX,0xXX};
    CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA256        = {0xXX,0xXX};
    CipherSuite TLS_PSK_WITH_AES_256_CBC_SHA384        = {0xXX,0xXX};
    CipherSuite TLS_PSK_WITH_NULL_SHA256               = {0xXX,0xXX};
    CipherSuite TLS_PSK_WITH_NULL_SHA384               = {0xXX,0xXX};
    CipherSuite TLS_DHE_PSK_WITH_AES_128_CBC_SHA256    = {0xXX,0xXX};
    CipherSuite TLS_DHE_PSK_WITH_AES_256_CBC_SHA384    = {0xXX,0xXX};
    CipherSuite TLS_DHE_PSK_WITH_NULL_SHA256           = {0xXX,0xXX};
    CipherSuite TLS_DHE_PSK_WITH_NULL_SHA384           = {0xXX,0xXX};
    CipherSuite TLS_RSA_PSK_WITH_AES_128_CBC_SHA256    = {0xXX,0xXX};
    CipherSuite TLS_RSA_PSK_WITH_AES_256_CBC_SHA384    = {0xXX,0xXX};
    CipherSuite TLS_RSA_PSK_WITH_NULL_SHA256           = {0xXX,0xXX};
    CipherSuite TLS_RSA_PSK_WITH_NULL_SHA384           = {0xXX,0xXX};
```

6. Acknowledgments

This draft borrows heavily from [RFC5289] and [RFC5288].

The author appreciates Alfred Hoenes for his detailed review and effort on issues resolving discussion. The author would like also to acknowledge Ibrahim Hajjeh, Simon Josefsson, Hassnaa Moustafa, Joseph Salowey and Pascal Urien for their reviews of the content of the document.

7. References

7.1. Normative References

[AES]   National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", FIPS 197, November 2001.

[CBC]   National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation - Methods and Techniques", SP 800-38A, December 2001.

[GCM]   National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication", SP 800-38D, November 2007.

   [SHS]   National Institute of Standards and Technology, "Secure
             Hash Standard", FIPS 180-2, August 2002.

   [RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-
             Hashing for Message Authentication", RFC 2104, February
             1997.

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

   [RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites
             for Transport Layer Security (TLS)", RFC 4279, December
             2005.

   [RFC4785] Blumenthal, U., Goel, P., "Pre-Shared Key (PSK)
             Ciphersuites with NULL Encryption for Transport Layer
             Security (TLS)", RFC 4785, January 2007.

   [RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated
             Encryption", RFC 5116, January 2008.

   [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security
             (TLS) Protocol Version 1.2", RFC 5246, August 2008.

   [RFC5288] Salowey, J., A. Choudhury, and C. McGrew, "RSA based AES-
             GCM Cipher Suites for TLS", RFC 5288, August 2008.

7.2. Informative References

   [RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-
             256/384 and AES Galois Counter Mode", RFC 5289, August
             2008.

   [Wang05] Wang, X., Yin, Y., and H. Yu, "Finding Collisions in the
             Full SHA-1", CRYPTO 2005, August 2005.

Author's Addresses

   Mohamad Badra
   LIMOS Laboratory - UMR6158, CNRS
   France

   Email: badra@isima.fr

Intellectual Property Statement

   The IETF takes no position regarding the validity or scope of any
   Intellectual Property Rights or other rights that might be claimed
   to pertain to the implementation or use of the technology described
   in this document or the extent to which any license under such
   rights might or might not be available; nor does it represent that
   it has made any independent effort to identify any such rights.
   Information on the procedures with respect to rights in RFC
   documents can be found in BCP 78 and BCP 79.

   Copies of IPR disclosures made to the IETF Secretariat and any
   assurances of licenses to be made available, or the result of an
   attempt made to obtain a general license or permission for the use
   of such proprietary rights by implementers or users of this
   specification can be obtained from the IETF on-line IPR repository
   at http://www.ietf.org/ipr.

   The IETF invites any interested party to bring to its attention any
   copyrights, patents or patent applications, or other proprietary
   rights that may cover technology that may be required to implement
   this standard. Please address the information to the IETF at
   ietf-ipr@ietf.org.

Disclaimer of Validity

   This document and the information contained herein are provided on
   an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE
   REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE
   IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL
   WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
   WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE
   ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS
   FOR A PARTICULAR PURPOSE.

Copyright Statement

   Copyright (C) The IETF Trust (2008).

   This document is subject to the rights, licenses and restrictions
   contained in BCP 78, and except as set forth therein, the authors
   retain all their rights.

Acknowledgment

   Funding for the RFC Editor function is currently provided by the
   Internet Society.