Network Working Group   E. Rescorla
Request for Comments: 5289   RTFM, Inc.
Category: Informational   August 2008

                TLS Elliptic Curve Cipher Suites with
            SHA-256/384 and AES Galois Counter Mode (GCM)

Status of This Memo

Abstract

   RFC 4492 describes elliptic curve cipher suites for Transport Layer
   Security (TLS). However, all those cipher suites use HMAC-SHA-1 as
   their Message Authentication Code (MAC) algorithm. This document
   describes sixteen new cipher suites for TLS that specify stronger MAC
   algorithms. Eight use Hashed Message Authentication Code (HMAC) with
   SHA-256 or SHA-384, and eight use AES in Galois Counter Mode (GCM).

Table of Contents

1. Introduction

   RFC 4492 [RFC4492] describes Elliptic Curve Cryptography (ECC) cipher
   suites for Transport Layer Security (TLS). However, all of the RFC
   4492 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. This document
   specifies TLS ECC cipher suites that use SHA-256 and SHA-384 [SHS]
   rather than SHA-1.

   TLS 1.2 [RFC5246], adds support for authenticated encryption with
   additional data (AEAD) cipher modes [RFC5116]. This document also
   specifies a set of ECC cipher suites using one such mode, Galois
   Counter Mode (GCM) [GCM]. Another document [RFC5288] provides
   support for GCM with other key establishment methods.

2. 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].

3. Cipher Suites

   This document defines 16 new cipher suites to be added to TLS. All
   use Elliptic Curve Cryptography for key exchange and digital
   signature, as defined in RFC 4492.

3.1. HMAC-Based Cipher Suites

   The first eight cipher suites use AES [AES] in Cipher Block Chaining
   (CBC) [CBC] mode with an HMAC-based MAC:

      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 = {0xC0,0x23};
      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 = {0xC0,0x24};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256   = {0xC0,0x25};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384   = {0xC0,0x26};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256   = {0xC0,0x27};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384   = {0xC0,0x28};
      CipherSuite TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256   = {0xC0,0x29};
      CipherSuite TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384   = {0xC0,0x2A};

   These eight cipher suites are the same as the corresponding cipher
   suites in RFC 4492 (with names ending in "_SHA" in place of "_SHA256"
   or "_SHA384"), except for the MAC and Pseudo Random Function (PRF)
   algorithms.

These SHALL be as follows:

o 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.

o 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. Galois Counter Mode-Based Cipher Suites

   The second eight cipher suites use the same asymmetric algorithms as
   those in the previous section but use the new authenticated
   encryption modes defined in TLS 1.2 with AES in Galois Counter Mode
   (GCM) [GCM]:

      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 = {0xC0,0x2B};
      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 = {0xC0,0x2C};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256   = {0xC0,0x2D};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384   = {0xC0,0x2E};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256   = {0xC0,0x2F};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   = {0xC0,0x30};
      CipherSuite TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256   = {0xC0,0x31};
      CipherSuite TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384   = {0xC0,0x32};

   These cipher suites use authenticated encryption with additional data
   algorithms AEAD_AES_128_GCM and AEAD_AES_256_GCM described in
   [RFC5116]. GCM is used as described in [RFC5288].

   The PRFs SHALL be as follows:

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

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

4. Security Considerations

   The security considerations in RFC 4346, RFC 4492, 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 these cipher suites:

      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256   = {0xC0,0x23};
      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384   = {0xC0,0x24};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256   = {0xC0,0x25};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384   = {0xC0,0x26};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256   = {0xC0,0x27};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384   = {0xC0,0x28};
      CipherSuite TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256   = {0xC0,0x29};
      CipherSuite TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384   = {0xC0,0x2A};
      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256   = {0xC0,0x2B};
      CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384   = {0xC0,0x2C};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256   = {0xC0,0x2D};
      CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384   = {0xC0,0x2E};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256   = {0xC0,0x2F};
      CipherSuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   = {0xC0,0x30};
      CipherSuite TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256   = {0xC0,0x31};
      CipherSuite TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384   = {0xC0,0x32};

6. Acknowledgements

   This work was supported by the US Department of Defense.

   David McGrew, Pasi Eronen, and Alfred Hoenes provided reviews of this
   document.

7. References

7.1. Normative References

   [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.

   [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, May 2006.

   [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., Choudhury, A., and D. McGrew, "AES-GCM Cipher
              Suites for TLS", RFC 5288, August 2008.

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

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

   [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.

7.2. Informative References

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

Author's Address

   Eric Rescorla
   RTFM, Inc.
   2064 Edgewood Drive
   Palo Alto 94303
   USA

   EMail: ekr@rtfm.com

Full Copyright Statement

Intellectual Property