Network Working Group
Internet-Draft
Intended status: Informational
Expires: October 31, 2008

E. Rescorla
RTFM, Inc.

April 29, 2008

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

draft-ietf-tls-ecc-new-mac-06.txt

Status of this Memo

Copyright Notice

Abstract

RFC 4492 describes elliptic curve cipher suites for Transport Layer Security (TLS). However, all those cipher suites use SHA-1 as their MAC algorithm. This document describes sixteen new CipherSuites for TLS/DTLS which specify stronger digest algorithms. Eight use 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 which use SHA-256 and SHA-384 rather than SHA-1.

TLS 1.2 [I-D.ietf-tls-rfc4346-bis], 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 [I-D.ietf-tls-rsa-aes-gcm], provides support for GCM with other key establishment methods.

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. Cipher Suites

This document defines 8 new cipher suites to be added to TLS. All use Elliptic Curve Cryptography for key exchange and digital signature, as defined in RFC 4492.

2.1. HMAC-based Cipher Suites

The first eight cipher suites use AES [AES] in CBC [CBC] mode with an HMAC-based MAC:

```
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256  = {0xXX,XX};
```

```
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384  = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256   = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384   = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256    = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384    = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256     = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384     = {0xXX,XX};
```

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 hash and PRF algorithms, which use SHA-256 and SHA-384 [SHS] as follows.

Cipher Suite	MAC	PRF
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA384

2.2. 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  = {0xXX,XX};
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384  = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256   = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384   = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256    = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384    = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256     = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384     = {0xXX,XX};
```

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 [I-D.ietf-tls-rsa-aes-gcm].

Cipher Suite	PRF
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	P_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	P_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	P_SHA384
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	P_SHA256
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	P_SHA384

3. Security Considerations

The security considerations in RFC 4346, RFC 4492, and [I-D.ietf-tls-rsa-aes-gcm] apply to this document as well. In

addition, as described in [I-D.ietf-tls-rsa-aes-gcm], these cipher suites may only be used with TLS 1.2 or greater.

4. IANA Considerations

IANA has assigned the following values for these cipher suites:

```
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256  = {0xXX,XX};
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384  = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256   = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384   = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256    = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384    = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256     = {0xXX,XX};
CipherSuite TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384     = {0xXX,XX};
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256  = {0xXX,XX};
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384  = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256   = {0xXX,XX};
CipherSuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384   = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256    = {0xXX,XX};
CipherSuite TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384    = {0xXX,XX};
```

```
      CipherSuite TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256     = {0xXX,XX};
      CipherSuite TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384     = {0xXX,XX};
```

5. Acknowledgements

This work was supported by the US Department of Defense.

David McGrew contributed substantual sections of the GCM nonce text as well as providing a review of this document.

6. References

6.1. Normative References

[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.

[I-D.ietf-tls-rfc4346-bis]
Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", draft-ietf-tls-rfc4346-bis-10 (work in progress), March 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.

6.2. Informative References

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

[I-D.ietf-tls-rsa-aes-gcm] Salowey, J., Choudhury, A., and D. McGrew, "AES-GCM Cipher Suites for TLS", draft-ietf-tls-rsa-aes-gcm-03 (work in progress), April 2008.

Author's Address

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

Email: ekr@rtfm.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).