TLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 23, 2011

D. McGrew
Cisco Systems, Inc.
D. Bailey
RSA/EMC
M. Campagna
R. Dugal
Certicom Corp.

January 19, 2011

AES-CCM ECC Cipher Suites for TLS
draft-mcgrew-tls-aes-ccm-ecc-01

Abstract

This memo describes the use of the Advanced Encryption Standard (AES) in the Counter and CBC-MAC Mode (CCM) of operation within Transport Layer Security (TLS) to provide confidentiality and data origin authentication. The AES-CCM algorithm is amenable to compact implementations, making it suitable for constrained environments. The ciphersuites defined in this document use Elliptic Curve Cryptography (ECC), and are intended for use in networks with limited bandwidth.

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 July 23, 2011.

Copyright Notice

(http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

This document describes the use of Advanced Encryption Standard (AES) [AES] in Counter with CBC-MAC Mode (CCM) [CCM] in several TLS ciphersuites. AES-CCM provides both authentication and confidentiality and uses as its only primitive the AES encrypt operation (the AES decrypt operation is not needed). This makes it amenable to compact implementations, which is advantageous in constrained environments. The use of AES-CCM has been specified for IPsec ESP [RFC4309] and 802.15.4 wireless networks [IEEE802154].

Authenticated encryption, in addition to providing confidentiality for the plaintext that is encrypted, provides a way to check its integrity and authenticity. Authenticated Encryption with Associated Data, or AEAD [RFC5116], adds the ability to check the integrity and authenticity of some associated data that is not encrypted. This note utilizes the AEAD facility within TLS 1.2 [RFC5246] and the AES-CCM-based AEAD algorithms defined in [RFC5116]. Additional AEAD algorithms are defined in this note; these use AES-CCM but have shorter authentication tags, and therefore are more suitable for use across networks in which bandwidth is constrained and message sizes may be small.

The ciphersuites defined in this document use Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) as their key establishment mechanism; these ciphersuites can be used with DTLS [I-D.ietf-tls-rfc4347-bis].

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. ECC based AES-CCM Cipher Suites

The ciphersuites defined in this document are based on the AES-CCM authenticated encryption with associated data (AEAD) algorithms AEAD_AES_128_CCM and AEAD_AES_256_CCM described in [RFC5116]. The following ciphersuites are defined:

```
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CCM = {TBD1,TBD1}
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CCM = {TBD2,TBD2)
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 = {TBD3,TBD3}
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 = {TBD4,TBD4)
```

These ciphersuites make use of the AEAD capability in TLS 1.2 [RFC5246]. Note that each of these AEAD algorithms uses AES-CCM. Ciphersuites ending with "8" use eight-octet authentication tags; the other ciphersuites have 16 octet authentication tags.

The HMAC truncation option described in Section 3.5 of [RFC4366] (which negotiates the "truncated_hmac" TLS extension) does not have an effect on the cipher suites defined in this note, because they do not use HMAC to protect TLS records.

The "nonce" input to the AEAD algorithm is defined as in [RFC5288]. The "nonce" SHALL be 12 bytes long and constructed as follows:

```
struct {
   case client:
      uint32 client_write_IV;  // low order 32-bits
   case server:
      uint32 server_write_IV;  // low order 32-bits
   uint64 seq_num;
} CCMNonce.
```

In DTLS, the 64-bit seq_num field is the 16-bit DTLS epoch field concatenated with the 48-bit sequence_number field. The epoch and sequence_number appear in the DTLS record layer.

This construction allows the internal counter to be 32-bits long, which is a convenient size for use with CCM.

These ciphersuites make use of the default TLS 1.2 Pseudorandom Function (PRF), which uses HMAC with the SHA-256 hash function.

The ECDHE_ECDSA key exchange is performed as defined in [RFC4492], with the following additional stipulations:

- The curves secp256r1 and secp384r1 MUST be supported, and the curve secp521r1 MAY be supported; these curves are equivalent to

the NIST P-256, P-384, and P-521 curves. Note that all of these curves have cofactor equal to one, which simplifies their use.

The server's certificate MUST contain an ECDSA-capable public key, it MUST be signed with ECDSA, and it MUST use SHA-256, SHA-384, or SHA-512. The Signature Algorithms extension (Section 7.4.1.4.1 of [RFC5246]) MUST be used to indicate support of those signature and hash algorithms. If a client certificate is used, the same conditions apply to it. The acceptable choices of hashes and curves that can be used with each ciphersuite are detailed in Section 2.1.

The uncompressed point format MUST be supported. Other point formats MAY be used.

The client MUST offer the elliptic_curves extension and the server MUST expect to receive it.

The client MAY offer the ec_point_formats extension, but the server need not expect to receive it.

[I-D.mcgrew-fundamental-ecc] MAY be used as an implementation method.

Implementations of these ciphersuites will interoperate with [RFC4492], but can be more compact than a full implementation of that RFC.

2.1. Required Algorithms for each CipherSuite

The curves and hash algorithms that can be used with each ciphersuite are described in the following table.

CipherSuite	Algorithms
TLS_ECDHE_ECDSA_WITH_AES_128_CCM	MUST support
TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	secp256r1, SHA-256
	MAY support
	secp384r1, SHA-384
	MAY support
	secp521r1, SHA-512
TLS_ECDHE_ECDSA_WITH_AES_256_CCM	MUST support
TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	secp384r1, SHA-384

	MAY support secp521r1, SHA-512

3. TLS Versions

These ciphersuites make use of the authenticated encryption with additional data defined in TLS 1.2 [RFC5288]. They MUST NOT be negotiated in older versions of TLS. 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. Because TLS has no way for the client to indicate that it supports TLS 1.2 but not earlier, a non-compliant server might potentially negotiate TLS 1.1 or earlier and select one of the cipher suites in this document. Clients MUST check the TLS version and generate a fatal "illegal_parameter" alert if they detect an incorrect version.

4. New AEAD algorithms

The following AEAD algorithms are defined:

```
AEAD_AES_128_CCM_8 = TBD9
AEAD_AES_256_CCM_8 = TBD10
AEAD_AES_128_CCM_12 = TBD11
AEAD_AES_256_CCM_12 = TBD12
```

4.1. AES-128-CCM with an 8-octet ICV

The AEAD_AES_128_CCM_8 authenticated encryption algorithm is identical to the AEAD_AES_128_CCM algorithm (see Section 5.3 of [RFC5116]), except that it uses eight octets for authentication, instead of the full sixteen octets used by AEAD_AES_128_CCM. The AEAD_AES_128_CCM_8 ciphertext consists of the ciphertext output of the CCM encryption operation concatenated with the 8-octet authentication tag output of the CCM encryption operation. Test cases are provided in [CCM]. The input and output lengths are as for AEAD_AES_128_CCM. An AEAD_AES_128_CCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

4.2. AES-256-CCM with an 8-octet ICV

The AEAD_AES_256_CCM_8 authenticated encryption algorithm is identical to the AEAD_AES_256_CCM algorithm (see Section 5.4 of [RFC5116]), except that it uses eight octets for authentication, instead of the full sixteen octets used by AEAD_AES_256_CCM. The AEAD_AES_256_CCM_8 ciphertext consists of the ciphertext output of the CCM encryption operation concatenated with the 8-octet authentication tag output of the CCM encryption operation. Test cases are provided in [CCM]. The input and output lengths are as for AEAD_AES_128_CCM. An AEAD_AES_128_CCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

5. IANA Considerations

IANA has assigned values for the Ciphersuites defined in Section 2 and the AEAD algorithms defined in Section 4 of this note.

6. Security Considerations

6.1. Perfect Forward Secrecy

The perfect forward secrecy properties of ephemeral Diffie-Hellman ciphersuites are discussed in the security analysis of [RFC4346]. This analysis applies to the ECDHE ciphersuites.

6.2. Counter Reuse

AES-CCM security requires that the counter is never reused. The IV construction in Section 2 is designed to prevent counter reuse.

7. Acknowledgements

This draft borrows heavily from [RFC5288].

This draft is motivated by the considerations raised in the Zigbee Smart Energy 2.0 working group.

8. References

8.1. Normative References

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

[CCM] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", SP 800-38C, May 2004.

[I-D.ietf-tls-rfc4347-bis] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security version 1.2", draft-ietf-tls-rfc4347-bis-03 (work in progress), October 2009.

[I-D.mcgrew-fundamental-ecc] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", draft-mcgrew-fundamental-ecc-04 (work in progress), December 2010.

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

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006.

[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 Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, August 2008.

8.2. Informative References

[IEEE802154] Institute of Electrical and Electronics Engineers, "Wireless Personal Area Networks", IEEE Standard 802.15.4-2006, 2006.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

Authors' Addresses

David McGrew
Cisco Systems, Inc.
170 W Tasman Drive
San Jose, CA 95134
USA

Email: mcgrew@cisco.com

Daniel V. Bailey
RSA/EMC
174 Middlesex Tpke.
Bedford, MA 01463
USA

Email: dbailey@rsa.com

Matthew Campagna
Certicom Corp.
5520 Explorer Drive #400
Mississauga, Ontario L4W 5L1
Canada

Email: mcampagna@certicom.com

Robert Dugal
Certicom Corp.
5520 Explorer Drive #400
Mississauga, Ontario L4W 5L1
Canada

Email: rdugal@certicom.com