TLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 30, 2015

A. Zauner
Independent

January 26, 2015

AES-OCB (Offset Codebook Mode) Ciphersuites for Transport Layer Security (TLS)

draft-zauner-tls-aes-ocb-02

Abstract

This memo describes the use of the Advanced Encryption Standard (AES) in the Offset Codebook Mode (OCB) of operation within Transport Layer Security (TLS) and Datagram TLS (DTLS) to provide confidentiality and data origin authentication. The AES-OCB algorithm is highly parallelizable, provable secure and can be efficiently implemented in software and hardware providing high performance.

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 30, 2015.

Table of Contents

1. Introduction

This document describes the use of the Advanced Encryption Standard (AES) in the Offset Codebook Mode (OCB) of operation within Transport Layer Security (TLS) and Datagram TLS (DTLS) to provide confidentiality and data origin authentication. The AES-OCB algorithm is highly parallelizable, provable secure and can be efficiently implemented in software and hardware providing high performance.

Furthermore OCB Mode [OCB] for AES [AES] provides a high performance, constant-time AEAD alternative to existing and deployed block-cipher modes without the need for special plattform specific instructions.

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 document utilizes the AEAD facility within TLS 1.2 [RFC5246] and the AES-OCB-based AEAD algorithms defined in [RFC5116] and [RFC7253].

The ciphersuites defined in this document use ECDHE, DHE or Pre-Shared-Key (PSK) as their key establishment mechanism; these ciphersuites can be used with DTLS [RFC6347]. Since the abiltiy to use AEAD ciphers was introduced in DTLS version 1.2, the ciphersuites

defined in this document cannot be used with earlier versions of that protocol.

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. Forward-secret AES-OCB Ciphersuites

The ciphersuites defined in this document are based on the AES-OCB authenticated encryption with associated data (AEAD) algorithms AEAD_AES_128_OCB_TAGLEN96 and AEAD_AES_256_OCB_TAGLEN96 described in [RFC7253]. The following forward-secret ciphersuites are defined:

```
CipherSuite TLS_DHE_RSA_WITH_AES_128_OCB = {TBD1, TBD1}
CipherSuite TLS_DHE_RSA_WITH_AES_256_OCB = {TBD2, TBD2}
CipherSuite TLS_ECDHE_RSA_WITH_AES_128_OCB = {TBD3, TBD3}
CipherSuite TLS_ECDHE_RSA_WITH_AES_256_OCB = {TBD4, TBD4}
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_OCB = {TBD5, TBD5}
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_OCB = {TBD6, TBD6}
```

These ciphersuites make use of the AEAD capability in TLS 1.2 [RFC5246].

Use of HMAC truncation in TLS (as specified in [RFC6066]) has no effect on the ciphersuites defined in this document.

The "nonce" input to the AEAD algorithm is exactly that of [RFC5288]: the "nonce" SHALL be 12 bytes long and is 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;
} OCBNonce.
```

The nonce input to the AEAD is described above using the TLS presentation language. All values are represented in big-endian form when constructing the AEAD input.

The sequence number of a message is always known to the receiver through other means (either implicit protocol state or a per-message header in the case of DTLS), so the nonce construction used does not

require any extra per-message information. Thus the record_iv_length is zero (0) for all ciphersuites defined in this document.

In DTLS, the 64-bit seq_num is the 16-bit epoch concatenated with the 48-bit seq_num.

These ciphersuites make use of the default TLS 1.2 Pseudorandom Function (PRF), which uses HMAC with the SHA-256 hash function. The ECDSA-ECDHE, RSA-ECDHE and RSA-DHE key exchanges are performed as defined in [RFC5246].

4. Pre-Shared-Key (PSK) AES-OCB Ciphersuites

As in Section 3, these ciphersuites follow [RFC7253]. The PSK, ECDHE_PSK and DHE_PSK key exchanges are performed as specified in [RFC4279]. The following Pre-Shared-Key (PSK) ciphersuites are defined:

```
CipherSuite TLS_PSK_WITH_AES_128_OCB = {TBD7, TBD7}
CipherSuite TLS_PSK_WITH_AES_256_OCB = {TBD8, TBD8}
CipherSuite TLS_DHE_PSK_WITH_AES_128_OCB = {TBD9, TBD9}
CipherSuite TLS_DHE_PSK_WITH_AES_256_OCB = {TBD10, TBD10}
CipherSuite TLS_ECDHE_PSK_WITH_AES_128_OCB = {TBD11, TBD11}
CipherSuite TLS_ECDHE_PSK_WITH_AES_256_OCB = {TBD12, TBD12}
```

The "nonce" input to the AEAD algorithm is identical to the one defined in Section 3. These ciphersuites make use of the default TLS 1.2 Pseudorandom Function (PRF), which uses HMAC with the SHA-256 hash function.

5. Applicable TLS Versions

These ciphersuites make use of the authenticated encryption with additional data (AEAD) defined in TLS 1.2 [RFC5288]. Earlier versions of TLS do not have support for AEAD; for instance, the TLSCiphertext structure does not have the "aead" option in TLS 1.1. Consequently, these ciphersuites 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 ciphersuites. 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.

6. IANA Considerations

IANA is requested to assign the values for the ciphersuites defined in Section 3 and Section 4 from the TLS and DTLS Ciphersuite registries. IANA, please note that the DTLS-OK column should be marked as "Y" for each of these algorithms.

7. Security Considerations

The security considerations in [RFC5246] apply to this document as well. The remainder of this section describes security considerations specific to the ciphersuites described in this document.

7.1. (Perfect) Forward Secrecy

With the exception of two Pre-Shared-Key (PSK) ciphersuites, defined in Section 4, this document deals exclusively with ciphersuites that are inherently forward-secret.

7.2. RSA as key-exchange

No ciphersuite is defined in this document that makes use of RSA as key-exchange.

7.3. Nonce reuse

AES-OCB security requires that the "nonce" (number used once) is never reused. The IV construction in Section 3 is designed to prevent nonce reuse.

8. Acknowledgements

This document borrows heavily from [RFC5288] and [RFC6655].

The author would like to thank Martin Thompson for his suggested change on the client negotiation paragraph, Nikos Mavrogiannopoulos and Peter Gutmann for the discussion on PSK ciphersuites, Jack Lloyd for content on the clarification of the TLS Record IV length and the TLS Working Group in general for feedback and discussion on this document.

9. References

9.1. Normative References

[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.

[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.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, July 2012.

9.2. Informative References

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

[OCB] Rogaway, P., Bellare, M., and J. Black, "OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption", CCS01 ACM Conference on Computer and Communications Security (CCS '01), ACM Press, pp. 196-205, 2001.

[RFC7253] Krovetz, T. and P. Rogaway, "The OCB Authenticated-Encryption Algorithm", RFC 7253, May 2014.

Author's Address

Aaron Zauner
Independent

Email: azet@azet.org