TLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 6, 2016

A. Zauner
lambda: resilient.systems

April 04, 2016

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

draft-zauner-tls-aes-ocb-04

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. Furthermore, use of AES-OCB in TLS is exempt from former IPR claims by various parties.

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 October 6, 2016.

Copyright Notice

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, single-pass, constant-time AEAD alternative to existing and deployed block-cipher modes without the need for special platform 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].

Because this document makes use of an AEAD construct, use of HMAC truncation in TLS (as specified in [RFC6066]) has no effect on the ciphersuites defined herein.

The "nonce" construction is identical to that of draft-ietf-tls-chacha20-poly1305-04:

AES-OCB requires a 96-bit nonce, which is formed as follows:

1. The 64-bit record sequence number is serialized as an 8-byte, big-endian value and padded on the left with four 0x00 bytes.

2. The padded sequence number is XORed with the client_write_IV (when the client is sending) or server_write_IV (when the server is sending).

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

This nonce construction is different from the one used with AES-GCM in TLS 1.2 but matches the scheme expected to be used in TLS 1.3. The nonce is constructed from the record sequence number and shared secret, both of which are known to the recipient. The advantage is that no per-record, explicit nonce need be transmitted, which saves eight bytes per record and prevents implementations from mistakenly using a random nonce. Thus, in the terms of [RFC5246], SecurityParameters.fixed_iv_length is twelve bytes and SecurityParameters.record_iv_length is zero bytes.

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 associated 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. Intellectual Property Rights

Historically Offset Codebook Mode has seen difficulty with implementation, deployment and standardization because of pending patents and intellectual rights claims on OCB itself. In preparation of this document all involved parties have declared they will issue IPR statements exempting use of OCB Mode in TLS from these claims. Specifically - OCB Mode as described in this document for use in TLS - is based, and strongly influenced, by earlier work from Charanjit Jutla on [IAPM].

6.1. Resolved IPR Claims

The following parties have made IPR claims in the past:

- US Patent No. 7,093,126 (Issued Aug 15, 2006) - Filed Apr 14, 2000. Inventor Name: Charanjit S. Jutla, Assignee: IBM
- US Patent No. 6,963,976 (Issued Nov 8, 2005) - Filed Nov 3, 2000. Inventor Name: Charanjit S. Jutla, Assignee: IBM
- US Patent No. 7,046,802 (Issued May 16, 2006) - Filed 30 Jul 2001. Inventor Name: Phillip W. Rogaway, Assignee: Rogaway Phillip W
- US Patent No. 7,200,227 (Issued Apr 3, 2007) - Filed 18 Jul 2005. Inventor Name: Phillip Rogaway, Assignee: Phillip Rogaway
- US Patent No. 7,949,129 (Issued May 24, 2011) - Filed 23 Mar 2007. Inventor Name: Phillip W. Rogaway, Assignee: Rogaway Phillip W

Use of technology described by these patents, when used with TLS, has been explicitly exempted from any previous claims by the original authors and patent holders.

7. 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.

8. 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.

8.1. (Perfect) Forward Secrecy

With the exception of two Pre-Shared-Key (PSK) ciphersuites intended for use in constrained environments and embedded devices (IoT), defined in Section 4, this document deals exclusively with ciphersuites that are inherently forward-secret.

8.2. Static RSA Key-transport

No ciphersuite is defined in this document that makes use of RSA as Key-Transport.

8.3. 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. Specifically, if there is any error in the nonce construction implementation, it will simply be non-interoperable with conforming implementations.

8.4. Data volume limit under a single key

There is a limitation on the total number of bytes that can be transmitted under one set of keys. For the AES-OCB ciphersuites, implementations MUST NOT transmit more than 2^36 bytes encrypted under a single key: they MUST rekey or close the connection before 2^36 bytes are reached. These limitations are based on limitations introduced in the TLS 1.3 draft for AES-GCM, this document adheres to the same constraints. A detailed analysis can be found in [AELIMIT].

9. Acknowledgements

This document borrows heavily from [RFC5288], [RFC6655] and draft-ietf-tls-chacha20-poly1305-04.

The author would like to thank Martin Thomson 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, Samuel Neves for suggesting the data-limitation paragraph from the TLS 1.3 draft and the TLS Working Group in general for feedback and discussion on this document.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC4279] Eronen, P., Ed. and H. Tschofenig, Ed., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, DOI 10.17487/RFC4279, December 2005, <http://www.rfc-editor.org/info/rfc4279>.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, DOI 10.17487/RFC5116, January 2008, <http://www.rfc-editor.org/info/rfc5116>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, DOI 10.17487/RFC5288, August 2008, <http://www.rfc-editor.org/info/rfc5288>.

[RFC6066] Eastlake 3rd, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, DOI 10.17487/RFC6066, January 2011, <http://www.rfc-editor.org/info/rfc6066>.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <http://www.rfc-editor.org/info/rfc6347>.

[RFC7253] Krovetz, T. and P. Rogaway, "The OCB Authenticated-Encryption Algorithm", RFC 7253, DOI 10.17487/RFC7253, May 2014, <http://www.rfc-editor.org/info/rfc7253>.

10.2. Informative References

[AELIMIT] Luykx, A. and K. Paterson, "Limits on Authenticated Encryption Use in TLS", date 2016-03-08, n.d..

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

[IAPM] Jutla, C., "Encryption Modes with Almost Free Message Integrity", EUROCRYPT01 Proc. Eurocrypt 2001, pp. 529-544, 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 2001), ACM Press, pp. 196-205, date 2001, n.d..

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, DOI 10.17487/RFC6655, July 2012, <http://www.rfc-editor.org/info/rfc6655>.

Author's Address

Aaron Zauner
lambda: resilient.systems

Email: azet@azet.org