Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 14, 2014

N. Williams
Cryptonector
March 13, 2014

Anonymous ECDH Ciphersuites with Modern Ciphers and Cipher Modes for Transport Layer Security (TLS)
draft-williams-tls-anon-ecdh-modern-cipher-01

Abstract

This document requests the registration and allocation of codepoints for new Transport Layer Security (TLS) ciphersuites with modern ciphers and cipher modes.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction and Motivation

The Transport Layer Security (TLS) [RFC5246] protocol supports a mode where key exchange is done without authenticating either the client nor the server to each other. This is done with ciphersuites using "anonymous" key agreement algorithms.

TLS ciphersuites are distinct sets of key agreement, server authentication, data encryption and integrity protection ciphers (and cipher modes), and pseudo-random functions (PRF). Each set that one might desire to use must be registered in the IANA TLS ciphersuite registry.

In recent years new, more modern ciphersuites have been added, but none with support for Elliptic Curve Diffie-Hellman (ECDH) [RFC4492] key agreement algorithms. This is problematic because ECDH is more efficient (both, in terms of compute and network bandwidth resources), and is generally thought to be more secure than the alternative. Thus implementations that want anonymous connections must trade-off security and performance in key agreement for security and performance in data encryption and integrity protection.

Note that there are good reasons to use anonymous ciphersuites, such as:

- to protect against passive attackers even when there's no way to authenticate the peer;

- to protect the identity of the server and/or the identity of the server as requested by the client in the server name indication (SNI) TLS extension -- here the client initiates a renegotiation with the protection of the outer, unauthenticated connection.

This is not an exhaustive list.

This document requests the allocation -and registration- of ciphersuite codepoints for at least some of the missing ciphersuites, specifically, the sets of ciphersuites resulting from the cartesian product of:

- ECDH for key agreement, with ephemeral keys

- no server authentication

- Advanced Encryption Standard (AES) [AES] for data encryption with the following key sizes:

   - 128-bit keys

   - 256-bit keys

- Two block cipher modes for authenticated encryption with additional data (AEAD):

   - Counter with CBC-MAC Mode (CCM) [RFC3610] [CCM]

   - Galois Counter Mode [GCM]

- Two hash functions for the TLS PRF:

   - SHA256 [RFC4634]

   - SHA384 [RFC4634]

filtered such that block cipher key lengths are matched to PRF hash functions as follows:

- 128-bit key-length ciphers should use SHA256 for the PRF

- 256-bit key-length ciphers should use SHA384 for the PRF

That's four new ciphersuites, see Section 3.

[[anchor1: Should such ciphersuites for Camellia and other alternative block ciphers also be registered by this document?]]

2. Security Considerations

There are no new security considerations here beyond those that are described in each of the documents normatively referenced here.

3. IANA Considerations

Pursuant to the TLS ciphersuite registry's allocation policy (Standards Action or Specification Required [RFC2434]), upon IESG Standards Action publishing this document on the Proposed Standards track, or acceptance by the RFC-Editor of this document for publication on the Informational track, the IANA should assign ciphersuite codepoints to the following ciphersuites, and add them to the TLS ciphersuite registry:

TLS_ECDH_anon_WITH_AES_128_GCM_SHA256 This is anonymous key agreement with ephemeral ECDH keys, with AES-128 in GCM mode, and SHA256 as the hash function for the TLS PRF.

TLS_ECDH_anon_WITH_AES_128_CCM_SHA256 This is anonymous key agreement with ephemeral ECDH keys, with AES-128 in CCM mode, and SHA256 as the hash function for the TLS PRF.

TLS_ECDH_anon_WITH_AES_256_GCM_SHA384 This is anonymous key agreement with ephemeral ECDH keys, with AES-256 in GCM mode, and SHA384 as the hash function for the TLS PRF.

TLS_ECDH_anon_WITH_AES_256_CCM_SHA384 This is anonymous key agreement with ephemeral ECDH keys, with AES-256 in CCM mode, and SHA384 as the hash function for the TLS PRF.

4. Normative References

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC2434] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[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.

[RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003.

[RFC4634] Eastlake, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, July 2006.

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

[GCM] Dworkin, M., "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication", Special Publication 800-38D, November 2007, <http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf>.

[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.

Author's Address

Nicolas Williams
Cryptonector, LLC

Email: nico@cryptonector.com