Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 15, 2008

E. Rescorla
RTFM, Inc.

February 12, 2008

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

draft-ietf-tls-ecc-new-mac-04.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 eight new CipherSuites for TLS/DTLS which specify stronger digest algorithms. Four use HMAC with SHA-256 or SHA-384 and four 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 replace 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 [I-D.mcgrew-auth-enc]. This document also specifies a set of ECC cipher suites using one such mode, Galois Counter Mode (GCM) [GCM]. Another document [I-D.salowey-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 four 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};
```

These four cipher suites are the same as the corresponding cipher suites in RFC 4492 (TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA, and TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA) except for the hash and PRF algorithms, which are SHA-256 and SHA-384 [SHS] as follows.

Cipher Suite	MAC	PRF
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA-256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA-384
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	HMAC-SHA-256	P_SHA-256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	HMAC-SHA-384	P_SHA-384

2.2. Galois Counter Mode-based Cipher Suites

The second four cipher suites 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};
```

These cipher suites use authenticated encryption with additional data algorithms AEAD_AES_128_GCM and AEAD_AES_256_GCM described in [I-D.mcgrew-auth-enc]. The "nonce" input to the AEAD algorithm SHALL be 12 bytes long, and is "partially implicit" (see Section 3.2.1 of [I-D.mcgrew-auth-enc]). Part of the nonce is generated as part of the handshake process and is static for the entire session and part is carried in each packet.

```
struct {
   opaque salt[4];
   opaque explicit_nonce_part[8];
} GCMNonce.
```

The salt value is either the client_write_IV if the client is sending or the server_write_IV if the server is sending. These IVs SHALL be 4 bytes long. Therefore, for all the algorithms defined in this section, SecurityParameters.fixed_iv_length=4.

The explicit_nonce_part is chosen by the sender and included in the packet. Each value of the explicit_nonce_part MUST be distinct from all other values, for any fixed key. Failure to meet this uniqueness requirement can significantly degrade security. The explicit_nonce_part is carried in the IV field of the GenericAEADCipher structure. Therefore, for all the algorithms defined in this section, SecurityParameters.record_iv_length=8.

In the case of TLS the counter MAY be the 64-bit sequence number. In the case of Datagram TLS [RFC4347] the counter MAY be formed from the concatenation of the 16-bit epoch with the 48-bit sequence number.

The PRF algorithms SHALL be as follows:

For TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 it SHALL be P_SHA-256.

For TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384 and TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA384 it SHALL be P_SHA-384.

3. TLS Versions

Because these cipher suites depend on features available only in TLS 1.2 (PRF flexibility and combined authenticated encryption cipher modes), they MUST NOT be negotiated by 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. Security Considerations

The security considerations in RFC 4346 and RFC 4492 apply to this document as well. The remainder of this section describes security considerations specific to the cipher suites described in this document.

4.1. Downgrade Attack

TLS negotiation is only as secure as the weakest cipher suite that is supported. For instance, an implementation which supports both 160-bit and 256-bit elliptic curves can be subject to an active downgrade attack to the 160-bit security level. An attacker who can attack that can then forge the Finished handshake check and successfully mount a man-in-the-middle attack.

4.2. Perfect Forward Secrecy

The static ECDH cipher suites specified in this document do not provide perfect forward secrecy (PFS). Thus, compromise of a single static key leads to potential decryption of all traffic protected using that key. Implementors of this specification SHOULD provide at least one ECDHE mode of operation.

4.3. Counter Reuse with GCM

AES-GCM is only secure if the counter is never reused. The IV construction algorithm above is designed to ensure that this cannot happen.

5. 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_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};
```

6. Acknowledgements

This work was supported by the US Department of Defense.

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

7. References

7.1. 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.

[I-D.mcgrew-auth-enc] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", draft-mcgrew-auth-enc-05 (work in progress), November 2007.

[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-09

(work in progress), February 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.

7.2. Informative References

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

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[I-D.salowey-tls-rsa-aes-gcm] Salowey, J., "RSA based AES-GCM Cipher Suites for TLS", draft-salowey-tls-rsa-aes-gcm-00 (work in progress), February 2007.

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).