TLS Working Group   Mohamad Badra
Internet Draft   LIMOS Laboratory
Intended status: Informational   July 28, 2008
Expires: December 2008

ECDHE_PSK Ciphersuites for Transport Layer Security (TLS)
draft-ietf-tls-ecdhe-psk-02.txt

Status of this Memo

Copyright Notice

Abstract

This document extends RFC 4279, RFC 4492 and RFC 4785, and specifies a set of ciphersuites that use a pre-shared key (PSK) to authenticate an Elliptic Curve Diffie-Hellman exchange (ECDH). These ciphersuites provide Perfect Forward Secrecy (PFS).

Table of Contents

1. Introduction

RFC 4279 specifies cipher suites for supporting TLS using pre-shared symmetric keys and they (a) use only symmetric key operations for authentication, (b) use a Diffie-Hellman exchange authenticated with a pre-shared key, or (c) combine public key authentication of the server with pre-shared key authentication of the client.

RFC 4785 specifies authentication-only cipher suites (with no encryption). These cipher suites are useful when authentication and integrity protection is desired, but confidentiality is not needed or not permitted.

RFC 4492 defines a set of ECC-based cipher suites for TLS and describes the use of ECC certificates for client authentication. In particular, it specifies the use of Elliptic Curve Diffie-Hellman (ECDH) key agreement in a TLS handshake and the use of Elliptic Curve Digital Signature Algorithm (ECDSA) as a new authentication mechanism.

This document specifies a set of cipher suites that use a PSK to authenticate an ECDH exchange. These cipher suites provide Perfect Forward Secrecy. One of these ciphersuites provides authentication-only.

The reader is expected to become familiar with RFC 4279, RFC 4492, and RFC 4785 prior to studying this document.

1.1. Applicability Statement

The ciphersuites defined in this document can be negotiated, whatever the negotiated TLS version

1.2. 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].

2. ECDHE_PSK Key Exchange Algorithm

The cipher suites in this section match the cipher suites defined in [RFC4279], except that they use an Elliptic Curve Diffie-Hellman exchange [RFC4492] authenticated with a PSK. They are defined as follow:

CipherSuite	Key Exchange	Cipher	Hash
TLS_ECDHE_PSK_WITH_RC4_128_SHA	ECDHE_PSK	RC4_128	SHA
TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA	ECDHE_PSK	3DES_EDE_CBC	SHA
TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA	ECDHE_PSK	AES_128_CBC	SHA
TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA	ECDHE_PSK	AES_256_CBC	SHA

These ciphersuites make use of the EC parameter negotiation mechanism defined in RFC 4492. When the ciphersuites defined in this document are used, the 'ec_diffie_hellman_psk' case inside the ServerKeyExchange and ClientKeyExchange structure MUST be used instead of the 'psk' case defined in [RFC4279] (i.e., the ServerKeyExchange and ClientKeyExchange messages include the Diffie-Hellman parameters). The PSK identity and identity hint fields have the same meaning and encoding as specified in [RFC4279] (note that the ServerKeyExchange message is always sent, even if no PSK identity hint is provided).

The format of the ServerKeyExchange and ClientKeyExchange messages is shown below.

```
struct {
    select (KeyExchangeAlgorithm) {
        /* other cases for rsa, diffie_hellman, etc. */
        case ec_diffie_hellman_psk:  /* NEW */
            opaque psk_identity_hint<0..2^16-1>;
            ServerECDHParams params;
    };
} ServerKeyExchange;

struct {
    select (KeyExchangeAlgorithm) {
        /* other cases for rsa, diffie_hellman, etc. */
        case ec_diffie_hellman_psk:   /* NEW */
            opaque psk_identity<0..2^16-1>;
            ClientECDiffieHellmanPublic public;
    } exchange_keys;
} ClientKeyExchange;
```

The premaster secret is formed as follows. First, perform the ECDH computation as described in Section 5.10 of [RFC4492]. Let Z be the octet string produced by this computation. Next, concatenate a uint16 containing the length of Z (in octets), Z itself, a uint16 containing the length of the PSK (in octets), and the PSK itself.

This corresponds to the general structure for the premaster secrets (see Note 1 in Section 2 of [RFC4279]), with "other_secret" containing Z.

```
struct {
     opaque other_secret<0..2^16-1>;
     opaque psk<0..2^16-1>;
};
```

3. ECDHE_PSK Key Exchange Algorithm with NULL Encryption

The cipher suite in this section matches the cipher suites defined in section 2, except that we define a suite with null encryption.

CipherSuite	Key Exchange	Cipher	Hash
TLS_ECDHE_PSK_WITH_NULL_SHA	ECDHE_PSK	NULL	SHA

4. Security Considerations

The security considerations described throughout [RFC4279], [ID-ietf-tls-rfc4346-bis], [RFC4492], and [RFC4785] apply here as well.

5. IANA Considerations

This document defines the following new cipher suites, whose values are to be assigned from the TLS Cipher Suite registry defined in [ID-ietf-tls-rfc4346-bis].

```
CipherSuite TLS_ECDHE_PSK_WITH_RC4_128_SHA        = { 0xXX, 0xXX };
CipherSuite TLS_ECDHE_PSK_WITH_3DES_EDE_CBC_SHA   = { 0xXX, 0xXX };
CipherSuite TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA    = { 0xXX, 0xXX };
CipherSuite TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA    = { 0xXX, 0xXX };
CipherSuite TLS_ECDHE_PSK_WITH_NULL_SHA           = { 0xXX, 0xXX };
```

6. Acknowledgments

The author would like to thank Bodo Moeller, Simon Josefsson, Uri Blumenthal, Pasi Eronen, Alfred Hoenes, Paul Hoffman, Joseph Salowey, and the TLS mailing list members for their comments on the 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.

[RFC4279] Eronen, P. and H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[ID-ietf-tls-rfc4346-bis]
Dierks, T. and E. Rescorla, "The TLS Protocol Version 1.2", draft-ietf-tls-rfc4346-bis-10 (work in progress), March 2008.

[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.

[RFC4785] Blumenthal, U. and P. Goel, "Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC 4785, January 2007.

Author's Addresses

Mohamad Badra
LIMOS Laboratory - UMR6158, CNRS
France

Email: badra@isima.fr

Intellectual Property Statement

this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.