TLS Working Group
Internet-Draft
Expires: May 25, 2005

P. Eronen, Ed.
Nokia
H. Tschofenig, Ed.
Siemens
November 24, 2004

Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)
draft-ietf-tls-psk-04.txt

Status of this Memo

Copyright Notice

Abstract

This document specifies three sets of new ciphersuites for the Transport Layer Security (TLS) protocol to support authentication based on pre-shared keys. These pre-shared keys are symmetric keys, shared in advance among the communicating parties. The first set of ciphersuites uses only symmetric key operations for authentication. The second set uses a Diffie-Hellman exchange authenticated with a pre-shared key; and the third set combines public key authentication

of the server with pre-shared key authentication of the client.

1. Introduction

Usually TLS uses public key certificates [3] or Kerberos [12] for authentication. This document describes how to use symmetric keys (later called pre-shared keys or PSKs), shared in advance among the communicating parties, to establish a TLS connection.

There are basically two reasons why one might want to do this:

- First, TLS may be used in performance-constrained environments where the CPU power needed for public key operations is not available.

- Second, pre-shared keys may be more convenient from a key management point of view. For instance, in closed environments where the connections are mostly configured manually in advance, it may be easier to configure a PSK than to use certificates. Another case is when the parties already have a mechanism for setting up a shared secret key, and that mechanism could be used to "bootstrap" a key for authenticating a TLS connection.

This document specifies three sets of new ciphersuites for TLS. These ciphersuites use new key exchange algorithms, and re-use existing cipher and MAC algorithms from [3] and [2]. A summary of these ciphersuites is shown below.

CipherSuite	Key Exchange	Cipher	Hash
TLS_PSK_WITH_RC4_128_SHA	PSK	RC4_128	SHA
TLS_PSK_WITH_3DES_EDE_CBC_SHA	PSK	3DES_EDE_CBC	SHA
TLS_PSK_WITH_AES_128_CBC_SHA	PSK	AES_128_CBC	SHA
TLS_PSK_WITH_AES_256_CBC_SHA	PSK	AES_256_CBC	SHA
TLS_DHE_PSK_WITH_RC4_128_SHA	DHE_PSK	RC4_128	SHA
TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA	DHE_PSK	3DES_EDE_CBC	SHA
TLS_DHE_PSK_WITH_AES_128_CBC_SHA	DHE_PSK	AES_128_CBC	SHA
TLS_DHE_PSK_WITH_AES_256_CBC_SHA	DHE_PSK	AES_256_CBC	SHA
TLS_RSA_PSK_WITH_RC4_128_SHA	RSA_PSK	RC4_128	SHA
TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA	RSA_PSK	3DES_EDE_CBC	SHA
TLS_RSA_PSK_WITH_AES_128_CBC_SHA	RSA_PSK	AES_128_CBC	SHA

TLS_RSA_PSK_WITH_AES_256_CBC_SHA RSA_PSK AES_256_CBC SHA

The first set of ciphersuites (with PSK key exchange algorithm), defined in Section 2 use only symmetric key algorithms, and are thus especially suitable for performance-constrained environments.

The ciphersuites in Section 3 (with DHE_PSK key exchange algorithm) use a PSK to authenticate a Diffie-Hellman exchange. These ciphersuites protect against dictionary attacks by passive

eavesdroppers (but not active attackers), and also provide Perfect Forward Secrecy (PFS).

The third set of ciphersuites (with RSA_PSK key exchange algorithm), defined in Section 4, combine public key based authentication of the server (using RSA and certificates) with mutual authentication using a PSK.

1.1 Applicability statement

The ciphersuites defined in this document are intended for a rather limited set of applications, usually involving only a very small number of clients and servers. Even in such environments, other alternatives may be more appropriate.

If the main goal is to avoid PKIs, another possibility worth considering is to use self-signed certificates with public key fingerprints. Instead of manually configuring a shared secret in, for instance, some configuration file, a fingerprint (hash) of the other party's public key (or certificate) could be placed there instead.

It is also possible to use the SRP (Secure Remote Password) ciphersuites for shared secret authentication [14]. SRP was designed to be used with passwords, and incorporates protection against dictionary attacks. However, it is computationally more expensive than the PSK ciphersuites in Section 2.

1.2 Conventions used in this document

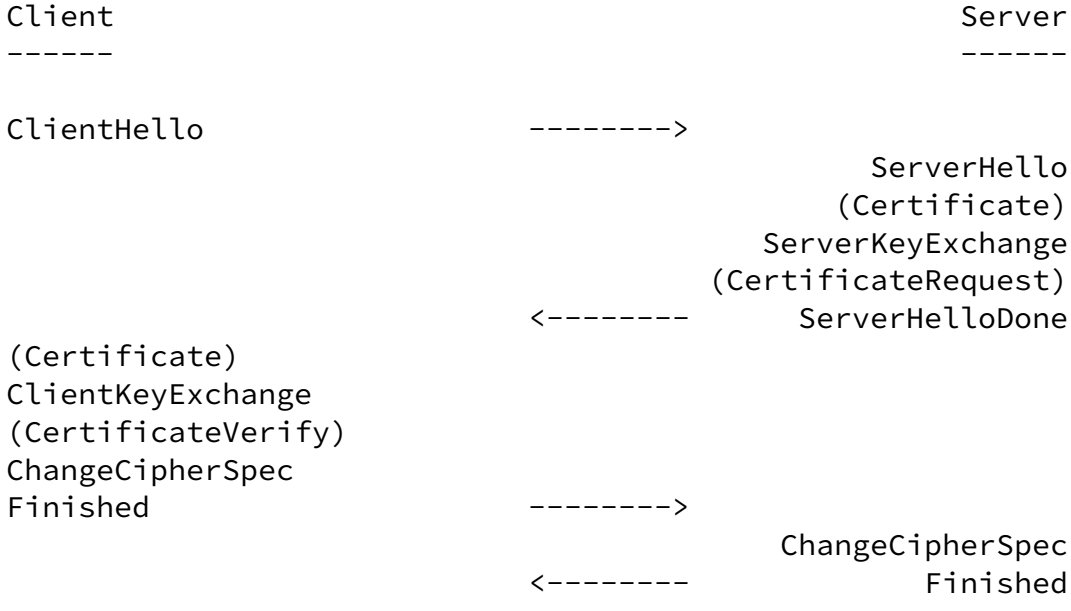
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

document are to be interpreted as described in [1].

2. PSK key exchange algorithm

This section defines the PSK key exchange algorithm and associated ciphersuites. These ciphersuites use only symmetric key algorithms.

It is assumed that the reader is familiar with ordinary TLS handshake, shown below. The elements in parenthesis are not included when PSK key exchange algorithm is used.



```
   Application Data            <------->     Application Data
```

The client indicates its willingness to use pre-shared key authentication by including one or more PSK ciphersuites in the ClientHello message. If the TLS server also wants to use pre-shared keys, it selects one of the PSK ciphersuites, places the selected ciphersuite in the ServerHello message, and includes an appropriate ServerKeyExchange message (see below). The Certificate and CertificateRequest payloads are omitted from the response.

Both clients and servers may have pre-shared keys with several different parties. The client indicates which key to use by including a "PSK identity" in the ClientKeyExchange message (note that unlike in [7], the session_id field in ClientHello message keeps its usual meaning). To help the client in selecting which identity to use, the server can provide a "PSK identity hint" in the ServerKeyExchange message (note that if no hint is provided, a ServerKeyExchange message is still sent).

It is expected that different types of identities are useful for different applications running over TLS. This document does not therefore mandate the use of any particular type of identity (such as

IPv4 address or FQDN) or identity hint; neither is specified how exactly the client uses the hint (if it uses it at all).

To increase the chances for successful interoperation between applications that do agree on what type of identity is used, the identity MUST be first converted to a character string, and then encoded to octets using UTF-8 [5]. For instance,

- IPv4 addresses are sent as dotted-decimal strings (e.g., "192.0.1.2"), not as 32-bit integers in network byte order.
- Domain names are sent in their usual text form (e.g., "www.example.com" or "embedded\.dot.example.net"), not in DNS protocol wire format.
- X.500 Distinguished Names are sent in their string representation [9], not as BER-encoded ASN.1.

In situations where the identity is entered by a person, processing the character string with an appropriate stringprep [10] profile is RECOMMENDED.

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

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

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


The premaster secret is formed as follows: if the PSK is N octets long, concatenate an uint16 with the value N, N zero octets, a second uint16 with the value N, and the PSK itself.

Note 1: All the ciphersuites in this document share the same general structure for the premaster secret, namely

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

Here "other_secret" is either zeroes (plain PSK case), or comes from the Diffie-Hellman or RSA exchange (DHE_PSK and RSA_PSK, respectively). See Sections 3 and 4 for a more detailed description.

Note 2: Using zeroes for "other_secret" effectively means that only the HMAC-SHA1 part (but not the HMAC-MD5 part) of the TLS PRF is used when constructing the master secret. See [8] for a more detailed rationale.

The TLS handshake is authenticated using the Finished messages as usual.

If the server does not recognize the PSK identity, it MAY respond with an "unknown_psk_identity" alert message. Alternatively, if the server wishes to hide the fact that the PSK identity was not known, it MAY continue the protocol as if the PSK identity existed but the key was incorrect: that is, respond with a "decrypt_error" alert.

3. DHE_PSK key exchange algorithm

This section defines additional ciphersuites that use a PSK to authenticate a Diffie-Hellman exchange. These ciphersuites give some

additional protection against dictionary attacks, and also provide Perfect Forward Secrecy (PFS). See Section 6 for discussion of related security considerations.

When these ciphersuites are used, the ServerKeyExchange and ClientKeyExchange also include the Diffie-Hellman parameters. The PSK identity and identity hint fields have the same meaning as in the previous section.

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

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

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

The premaster secret is formed as follows. Let Z be the value produced by the Diffie-Hellman exchange (with leading zero bytes stripped as in other Diffie-Hellman based ciphersuites). Concatenate an uint16 containing the length of Z (in octets), Z itself, an 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) in this document, with "other_secret" containing Z.

4. RSA_PSK key exchange algorithm

The ciphersuites in this section use RSA and certificates to authenticate the server, in addition to using a PSK.

As in normal RSA ciphersuites, the server must send a Certificate message. The format of the ServerKeyExchange and ClientKeyExchange messages is shown below.

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

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

The EncryptedPreMasterSecret field sent from the client to the server contains a 2-byte version number and a 46-byte random value, encrypted using the server's RSA public key as described in Section 7.4.7.1 of [3]. The actual premaster secret is formed by both parties as follows: concatenate an uint16 with the value 48, the 2-byte version number and the 46-byte random value, an 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) in this document, with "other_secret" containing both the 2-byte version number and the 46-byte random value.

Neither the normal RSA ciphersuites nor these RSA_PSK ciphersuites themselves specify what the certificates contain (in addition to the RSA public key), or how the certificates are to be validated. In particular, it is possible to use the RSA_PSK ciphersuites with unvalidated self-signed certificates to provide somewhat similar protection against dictionary attacks as the DHE_PSK ciphersuites defined in Section 3.

5. IANA considerations

IANA does not currently have a registry for TLS-related numbers, so there are no IANA actions associated with this document.

For easier reference in the future, the ciphersuite numbers defined in this document are summarized below.

```
CipherSuite TLS_PSK_WITH_RC4_128_SHA          = { 0x00, 0x8A };
CipherSuite TLS_PSK_WITH_3DES_EDE_CBC_SHA     = { 0x00, 0x8B };
CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA      = { 0x00, 0x8C };
CipherSuite TLS_PSK_WITH_AES_256_CBC_SHA      = { 0x00, 0x8D };
CipherSuite TLS_DHE_PSK_WITH_RC4_128_SHA      = { 0x00, 0x8E };
CipherSuite TLS_DHE_PSK_WITH_3DES_EDE_CBC_SHA = { 0x00, 0x8F };
CipherSuite TLS_DHE_PSK_WITH_AES_128_CBC_SHA  = { 0x00, 0x90 };
CipherSuite TLS_DHE_PSK_WITH_AES_256_CBC_SHA  = { 0x00, 0x91 };
CipherSuite TLS_RSA_PSK_WITH_RC4_128_SHA      = { 0x00, 0x92 };
CipherSuite TLS_RSA_PSK_WITH_3DES_EDE_CBC_SHA = { 0x00, 0x93 };
CipherSuite TLS_RSA_PSK_WITH_AES_128_CBC_SHA  = { 0x00, 0x94 };
CipherSuite TLS_RSA_PSK_WITH_AES_256_CBC_SHA  = { 0x00, 0x95 };
```

This document also defines a new TLS alert message, unknown_psk_identity(115).

6. Security Considerations

As with all schemes involving shared keys, special care should be taken to protect the shared values and to limit their exposure over time.

6.1 Perfect forward secrecy (PFS)

The PSK and RSA_PSK ciphersuites defined in this document do not provide Perfect Forward Secrecy (PFS). That is, if the shared secret key (in PSK ciphersuites), or both the shared secret key and the RSA private key (in RSA_PSK ciphersuites), is somehow compromised, an attacker can decrypt old conversations.

The DHE_PSK ciphersuites provide Perfect Forward Secrecy if a fresh DH private key is generated for each handshake.

6.2 Brute-force and dictionary attacks

Use of a fixed shared secret of limited entropy (for example, a PSK that is relatively short, or was chosen by a human and thus may contain less entropy than its length would imply) may allow an attacker to perform a brute-force or dictionary attack to recover the secret. This may be either an off-line attack (against a captured

TLS handshake messages), or an on-line attack where the attacker attempts to connect to the server and tries different keys.

For the PSK ciphersuites, an attacker can get the information required for an off-line attack by eavesdropping a TLS handshake, or by getting a valid client to attempt connection with the attacker (by tricking the client to connect to wrong address, or intercepting a connection attempt to the correct address, for instance).

For the DHE_PSK ciphersuites, an attacker can obtain the information by getting a valid client to attempt connection with the attacker. Passive eavesdropping alone is not sufficient.

For the RSA_PSK ciphersuites, only the server (authenticated using RSA and certificates) can obtain sufficient information for an off-line attack.

It is RECOMMENDED that implementations that allow the administrator to manually configure the PSK also provide a functionality for generating a new random PSK, taking [4] into account.

6.3 Identity privacy

The PSK identity is sent in cleartext. While using a user name or other similar string as the PSK identity is the most straightforward option, it may lead to problems in some environments since an eavesdropper is able to identify the communicating parties. Even when the identity does not reveal any information itself, reusing the same identity over time may eventually allow an attacker to perform traffic analysis to identify the parties. It should be noted that this is no worse than client certificates, since they are also sent in cleartext.

6.4 Implementation notes

The implementation notes in [11] about correct implementation and use of RSA (including Section 7.4.7.1) and Diffie-Hellman (including Appendix F.1.1.3) apply to the DHE_PSK and RSA_PSK ciphersuites as well.

7. Acknowledgments

The protocol defined in this document is heavily based on work by Tim Dierks and Peter Gutmann, and borrows some text from [7] and [2]. The DHE_PSK and RSA_PSK ciphersuites are based on earlier work in [6].

Valuable feedback was also provided by Philip Ginzboorg, Peter

Gutmann, David Jablon, Nikos Mavroyanopoulos, Bodo Moeller, Eric Rescorla, and Mika Tervonen.

When the first version of this draft was almost ready, the authors learned that something similar had been proposed already in 1996 [13]. However, this draft is not intended for web password authentication, but rather for other uses of TLS.

8. References

8.1 Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[2] Chown, P., "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", RFC 3268, June 2002.

[3] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[4] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

[5] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 3629, November 2003.

8.2 Informative References

[6] Badra, M., Cherkaoui, O., Hajjeh, I. and A. Serhrouchni, "Pre-Shared-Key key Exchange methods for TLS", draft-badra-tls-key-exchange-00 (work in progress), August 2004.

[7] Gutmann, P., "Use of Shared Keys in the TLS Protocol", draft-ietf-tls-sharedkeys-02 (expired), October 2003.

[8] Krawczyk, H., "Re: TLS shared keys PRF", message on ietf-tls@lists.certicom.com mailing list 2004-01-13, http://www.imc.org/ietf-tls/mail-archive/msg04098.html.

[9] Zeilenga, K., "LDAP: String Representation of Distinguished Names", draft-ietf-ldapbis-dn-15 (work in progress), October 2004.

[10] Hoffman, P. and M. Blanchet, "Preparation of Internationalized Strings ("stringprep")", RFC 3454, December 2002.

[11] Dierks, T. and E. Rescorla, "The TLS Protocol Version 1.1", draft-ietf-tls-rfc2246-bis-08 (work in progress), August 2004.

[12] Medvinsky, A. and M. Hur, "Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)", RFC 2712, October 1999.

[13] Simon, D., "Addition of Shared Key Authentication to Transport Layer Security (TLS)", draft-ietf-tls-passauth-00 (expired), November 1996.

[14] Taylor, D., Wu, T., Mavroyanopoulos, N. and T. Perrin, "Using SRP for TLS Authentication", draft-ietf-tls-srp-08 (work in progress), August 2004.

Authors' and Contributors' Addresses

Pasi Eronen
Nokia Research Center
P.O. Box 407
FIN-00045 Nokia Group
Finland
Email: pasi.eronen@nokia.com

Hannes Tschofenig
Siemens

Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany
Email: Hannes.Tschofenig@siemens.com

Mohamad Badra
ENST Telecom
46 rue Barrault
75634 Paris
France
Email: Mohamad.Badra@enst.fr

Omar Cherkaoui
UQAM University
Montreal (Quebec)
Canada
Email: cherkaoui.omar@uqam.ca

Ibrahim Hajjeh
ENST Telecom
46 rue Barrault
75634 Paris
France
Email: Ibrahim.Hajjeh@enst.fr

Ahmed Serhrouchni
ENST Telecom
46 rue Barrault
75634 Paris
France
Email: Ahmed.Serhrouchni@enst.fr

Appendix A. Changelog

(This section should be removed by the RFC Editor before publication.)

Changes from -03 to -04:

- Added a note about premaster secret "general structure" in Sections 3 and 4.

- Something in the I-D submission procedure had removed all circumflexes from -03 version, turning e.g. "2^16" (two-to-the sixteenth power) to "216" (two hundred and sixteen). Let's try again.

Changes from -02 to -03:

- Aligned the way the premaster secret is derived.

- Specified that identities must be sent as human-readable UTF-8 strings, not in binary formats. Changed reference to RFC 3629 from informative to normative.

- Selected ciphersuite and alert numbers, and updated IANA considerations section to match this.

- Reworded some text about dictionary attacks in Section 6.2.

Changes from -01 to -02:

- Clarified text about DHE_PSK ciphersuites in Section 1.

- Clarified explanation of HMAC-SHA1/MD5 use of PRF in Section 2.

- Added note about certificate validation and self-signed certificates in Section 4.

- Added Mohamad Badra et al. as contributors.

Changes from draft-ietf-tls-psk-00 to -01:

- Added DHE_PSK and RSA_PSK key exchange algorithms, and updated other text accordingly

- Removed SHA-1 hash from PSK key exchange premaster secret construction (since premaster secret doesn't need to be 48 bytes).

- Added unknown_psk_identity alert message.

- Updated IANA considerations section.

Changes from draft-eronen-tls-psk-00 to draft-ietf-tls-psk-00:

- Updated dictionary attack considerations based on comments from David Jablon.

- Added a recommendation about using UTF-8 in the identity field.

- Removed Appendix A comparing this document with draft-ietf-tls-sharedkeys-02.

- Removed IPR comment about SPR.

- Minor editorial changes.

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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