Network Working Group
Request for Comments: 4785
Category: Standards Track

U. Blumenthal
P. Goel
Intel Corporation

January 2007

Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)

Status of This Memo

Copyright Notice

Abstract

This document specifies authentication-only ciphersuites (with no encryption) for the Pre-Shared Key (PSK) based Transport Layer Security (TLS) protocol. These ciphersuites are useful when authentication and integrity protection is desired, but confidentiality is not needed or not permitted.

Table of Contents

1. Introduction

The RFC for Pre-Shared Key (PSK) based Transport Layer Security (TLS) [TLS-PSK] specifies ciphersuites for supporting TLS using pre-shared symmetric keys. However, all the ciphersuites defined in [TLS-PSK] require encryption. However there are cases when only authentication and integrity protection is required, and confidentiality is not needed. There are also cases when confidentiality is not permitted - e.g., for implementations that must meet import restrictions in some countries. Even though no encryption is used, these ciphersuites support authentication of the client and server to each other, and message integrity. This document augments [TLS-PSK] by adding three more ciphersuites (PSK, DHE_PSK, RSA_PSK) with authentication and integrity only - no encryption. The reader is expected to become familiar with [TLS-PSK] standards prior to studying this document.

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 Public-key Infrastructures (PKIs), another possibility worth considering is using 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 Secure Remote Password (SRP) ciphersuites for shared secret authentication [SRP]. SRP was designed to be used with passwords, and it incorporates protection against dictionary attacks. However, it is computationally more expensive than the PSK ciphersuites in [TLS-PSK].

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. Cipher Usage

The three new ciphersuites proposed here match the three cipher suites defined in [TLS-PSK], except that we define suites with null encryption.

The ciphersuites defined here use the following options for key exchange and hash part of the protocol:

CipherSuite	Key Exchange	Cipher	Hash
TLS_PSK_WITH_NULL_SHA	PSK	NULL	SHA
TLS_DHE_PSK_WITH_NULL_SHA	DHE_PSK	NULL	SHA
TLS_RSA_PSK_WITH_NULL_SHA	RSA_PSK	NULL	SHA

For the meaning of the terms PSK, please refer to section 1 in [TLS-PSK]. For the meaning of the terms DHE, RSA, and SHA, please refer to appendixes A.5 and B in [TLS].

4. 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. As this document augments [TLS-PSK], everything stated in its Security Consideration section applies here. In addition, as cipher suites defined here do not support confidentiality, care should be taken not to send sensitive information (such as passwords) over connections protected with one of the ciphersuites defined in this document.

5. IANA Considerations

This document defines three new ciphersuites whose values are in the TLS Cipher Suite registry defined in [TLS].

```
CipherSuite   TLS_PSK_WITH_NULL_SHA      = { 0x00, 0x2C };
CipherSuite   TLS_DHE_PSK_WITH_NULL_SHA  = { 0x00, 0x2D };
CipherSuite   TLS_RSA_PSK_WITH_NULL_SHA  = { 0x00, 0x2E };
```

6. Acknowledgments

The ciphersuites defined in this document are an augmentation to and based on [TLS-PSK].

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.

[TLS] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

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

7.2. Informative References

[SRP] Taylor, D., Wu, T., Mavrogiannopoulos, N., and T. Perrin, "Using SRP for TLS Authentication", Work in Progress, December 2006.

Authors' Addresses

Uri Blumenthal
Intel Corporation
1515 State Route 10,
PY2-1 10-4
Parsippany, NJ 07054
USA

EMail: urimobile@optonline.net

Purushottam Goel
Intel Corporation
2111 N.E. 25 Ave.
JF3-414
Hillsboro, OR 97124
USA

EMail: Purushottam.Goel@intel.com

Full Copyright Statement

Intellectual Property

Acknowledgement

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