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

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The IETF Trust (2007).

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 .................................................... 2
   1.1. Applicability Statement .................................. 2
2. Conventions Used in This Document ............................ 2
3. Cipher Usage .................................................. 3
4. Security Considerations ...................................... 3
5. IANA Considerations .......................................... 3
6. Acknowledgments .............................................. 3
7. References .................................................... 4
   7.1. Normative References .................................. 4
   7.2. Informative References ................................. 4
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:

<table>
<thead>
<tr>
<th>CipherSuite</th>
<th>Key Exchange</th>
<th>Cipher</th>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_PSK_WITH_NULL_SHA</td>
<td>PSK</td>
<td>NULL</td>
<td>SHA</td>
</tr>
<tr>
<td>TLS_DHE_PSK_WITH_NULL_SHA</td>
<td>DHE_PSK</td>
<td>NULL</td>
<td>SHA</td>
</tr>
<tr>
<td>TLS_RSA_PSK_WITH_NULL_SHA</td>
<td>RSA_PSK</td>
<td>NULL</td>
<td>SHA</td>
</tr>
</tbody>
</table>

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].

<table>
<thead>
<tr>
<th>CipherSuite</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS_PSK_WITH_NULL_SHA</td>
<td>0x00 0x2C</td>
</tr>
<tr>
<td>TLS_DHE_PSK_WITH_NULL_SHA</td>
<td>0x00 0x2D</td>
</tr>
<tr>
<td>TLS_RSA_PSK_WITH_NULL_SHA</td>
<td>0x00 0x2E</td>
</tr>
</tbody>
</table>

6. Acknowledgments

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

7.1. Normative References


7.2. Informative References


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