TLS Working Group
Internet Draft
Expires: April 2007

U. Blumenthal
P. Goel
Intel Corporation

October 20, 2006

Pre-Shared Key Cipher Suites with NULL Encryption for Transport Layer Security (TLS)

draft-ietf-tls-psk-null-03.txt

Status of this Memo

Abstract

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

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].

Table of Contents

1. Introduction

The RFC for Pre-Shared Key based TLS [TLS-PSK] specifies cipher suites for supporting TLS using pre-shared symmetric keys. However all the cipher suites 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 cipher suites support authentication of the client and server to each other, and message integrity. This document augments [TLS-PSK] by adding three more cipher suites (PSK, DHE_PSK, RSA_PSK) with authentication and integrity only - no encryption. The reader is expected to become familiar with [TLS-PSK] standard prior to studying this document.

2. Cipher Usage

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

The cipher suites 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 sections A.5 and Appendix B in [TLS].

3. 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 connection protected with one of the cipher suites defined in this document.

4. IANA Considerations

This document defines three new cipher suites, whose values are to be assigned from the TLS Cipher Suite registry defined in [TLS].

```
CipherSuite   TLS_PSK_WITH_NULL_SHA      = { 0x00, 0xTBD1 };
CipherSuite   TLS_DHE_PSK_WITH_NULL_SHA  = { 0x00, 0xTBD2 };
CipherSuite   TLS_RSA_PSK_WITH_NULL_SHA  = { 0x00, 0xTBD3 };
```

5. Acknowledgments

The cipher suites defined in this document are an augmentation to and

based on [TLS-PSK].

6. References

6.1. 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 Rescorla, E., "The TLS Protocol Version 1.1", RFC 4346, April 2006.

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

Author's Addresses

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

Email: Uri.Blumenthal@intel.com

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

Email: Purushottam.Goel@intel.com

Acknowledgment

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

Intellectual Property Statement

Disclaimer of Validity

WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement