TLS Working Group
Internet Draft
Expires: April 2007

U. Blumenthal
P. Goel
Intel Corporation

October 3, 2006

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

draft-ietf-tls-psk-null-02.txt

Status of this Memo

This Internet-Draft will expire on April 3, 2007.

Abstract

This document specifies authentication-only cipher suites for the Pre-Shared Key based Transport Layer Security (TLS) protocol to support null encryption. These cipher suites are useful for countries and places with cryptography-related restrictions.

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. There is a need for cipher suites that support no encryption. This is required for implementations to 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.

2. Cipher Usage

The new cipher suites proposed here is very similar to cipher suites defined in [TLS-PSK], except that they define 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 and RSA please refer to section 7.4.2 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

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has

made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement 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.