

Network Working Group
Hoffman
Internet-Draft
Consortium
Intended status: Standards Track
2010
Expires: August 2, 2010

P.
VPN
January 29,

**Additional Random Extension to TLS
draft-hoffman-tls-additional-random-ext-00**

Abstract

This document specifies a TLS/DTLS extension that uses the additional master secret inputs to achieve useful security properties.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 2, 2010.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

1. Introduction

This document defines a TLS [[RFC5246](#)] and DTLS [[RFC4347](#)] extension to provide additional random values for the derivation of the master_secret. This extension is a "extensions with master secret input" as defined in [[MASTERSECRETINPUT](#)].

1.1. 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](#)].

2. The additional_random Extension

TLS and DTLS use a 32-byte "Random" value consisting of a 32-bit time value and 28 randomly generated bytes. The client and server each contribute a Random value which is then mixed with secret keying material to produce the final per-association keying material. In some application environments, it is desirable to have the client and/or the server be able to input more random material in the master key calculation than is allowed by the fixed-length Random value.

The additional_random extension to TLS and DTLS adds a variable amount of client-specified and/or server-specified opaque randomness to the master key calculation.

The extension data field of the additional_random extension contains a Additional_Random_Data structure:

```
struct {  
    opaque additional_random_value<0..2^16>  
} Additional_Random_Data;
```

The additional_random_value is a single opaque random octet string. The recipient of an additional_random extension MUST NOT try to

parse
the additional_random_value.

Negotiating the additional_random extension has the same semantics as negotiating any other TLS/DTLS extension. In addition, the size of the additional_random_value provided by the client does not indicate anything about the expected size of the additional_random_value from the server.

The extension type for the additional_random extension is {TBD}.

The additional_random extension is a extension with master secret input as defined in [[MASTERSECRETINPUT](#)]. The entire extension (including the extension type {TBD}, the length value, and the Additional_Random_Data) is used as the additional_ms_input value for calculating the master secret.

3. Security Considerations

Adding greater entropy to the master secret calculation does not have any negative security impacts on the master secret.

4. IANA Considerations

This document defines an extension to TLS, in accordance with [RFC 4366](#). The following is to be added to the TLS Extensions registry (<http://www.iana.org/assignments/tls-extensiontype-values/> [tls-extensiontype-values.xhtml](#)):

```
enum { additional_random(TBD) }  
      ExtensionType;
```

5. Acknowledgements

Some of the ideas in this document came from earlier documents authored by Eric Rescorla, Margaret Salter, and Jerry Solinas.

6. Normative References

- [MASTERSECRETINPUT] Hoffman, P., "Additional Master Secret Inputs for TLS", [draft-hoffman-tls-master-secret-input](#) (work in progress), January 2010.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", [RFC 4347](#), April 2006.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 2008.

Author's Address

Paul Hoffman
VPN Consortium

Email: paul.hoffman@vpnc.org