                   Additional Random Extension to TLS
                  draft-hoffman-tls-additional-random-ext-01

Abstract

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

Status of this Memo

Copyright Notice

1. Introduction

This document defines a TLS 1.2 [RFC5246] and DTLS 1.2 [4347bis]
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.
For example, one peer might want to add session-specific public
entropy of a sufficient length for the chosen hash function to
influence all bits of the outcome in case the other peer has a
deficient entropy source.

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 extention 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 client and server MUST generate the additional_random_value data
using a secure random number generator; [RFC4086] gives guidance on
the generation of random values. 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. Specifically, the client is not requesting a particular
size of response 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 body of the extension,
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

Much of the text in this document is derived from text written by
Eric Rescorla, Margaret Salter, and Jerry Solinas.

6. Normative References

[4347bis]   Rescorla, E. and N. Modadugu, "Datagram Transport Layer
            Security version 1.2", draft-ietf-tls-rfc4347-bis (work in
            progress), October 2009.

[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.

[RFC4086] Eastlake, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

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

Appendix A. Differences between -00 and -01

[[This section to be removed before final publication.]]

Clarified that this extension applies only to TLS 1.2 and DTLS 1.2.

Added a clearer explanation of when the extension might be used: "For example, one peer might want to add session-specific public entropy of a sufficient length for the chosen hash function to influence all bits of the outcome in case the other peer has a deficient entropy source."

Changed what gets put into the master secret from "the entire extension" to "the body of the extension".

Added "The client and server MUST generate the additional_random_value data using a secure random number generator; [RFC4086] gives guidance on the generation of random values."

Author's Address

   Paul Hoffman
   VPN Consortium

   Email: paul.hoffman@vpnc.org