DTLS over DCCP
Internet Draft   T. Phelan
Document: draft-ietf-dccp-dtls-01.txt   Sonus Networks
Expires: February 2008   August 2007
Intended status: Proposed Standard

            Datagram Transport Layer Security (DTLS) over the Datagram
                   Congestion Control Protocol (DCCP)

   Status of this Memo

   By submitting this Internet-Draft, each author represents that any
   applicable patent or other IPR claims of which he or she is aware
   have been or will be disclosed, and any of which he or she becomes
   aware will be disclosed, in accordance with Section 6 of 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 September 30, 2007.

   Abstract

   This document specifies the use of Datagram Transport Layer Security
   (DTLS) over the Datagram Congestion Control Protocol (DCCP). DTLS
   provides communications privacy for datagram protocols and allows
   client/server applications to communicate in a way that is designed
   to prevent eavesdropping, tampering, or message forgery. DCCP is a
   transport protocol that provides a congestion-controlled unreliable
   datagram service.

Table of Contents

1. Introduction

   This document specifies how to use Datagram Transport Layer Security
   (DTLS), as specified in [RFC4347], over the Datagram Congestion
   Control Protocol (DCCP), as specified in [RFC4340].

   DTLS is an extension of Transport Layer Security (TLS, [RFC4346])
   that modifies TLS for use with the unreliable transport protocol UDP.
   TLS is a protocol that allows client/server applications to
   communicate in a way that is designed to prevent eavesdropping,
   tampering and message forgery. DTLS can be viewed as TLS-plus-
   adaptations-for-unreliability.

   DCCP provides an unreliable transport service, similar to UDP, but
   with adaptive congestion control, similar to TCP and SCTP. DCCP can
   be viewed equally well as either UDP-plus-congestion-control or TCP-
   minus-reliability (although, unlike TCP, DCCP offers multiple
   congestion control algorithms).

   The combination of DTLS and DCCP will offer transport security
   capabilities to DCCP users similar to those available for TCP, UDP
   and SCTP.

2. Terminology

   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 specified in [RFC2119].

3. DTLS over DCCP

   The approach here is very straightforward -- DTLS records are
   transmitted in the Application Data fields of DCCP-Data and DCCP-
   DataAck packets. Multiple DTLS records MAY be sent in one DCCP
   packet, as long as the resulting packet is within the Path Maximum
   Transfer Unit (PMTU) currently in force (see section 3.3 for more
   information on PMTU Discovery). A single DTLS record MUST be fully
   contained in a single DCCP packet; it MUST NOT be split over multiple
   packets.

3.1 DCCP and DTLS Sequence Numbers

   Both DCCP and DTLS use sequence numbers in their packets/records.
   These sequence numbers serve somewhat, but not completely,
   overlapping functions. Consequently, there is no connection between
   the sequence number of a DCCP packet and the sequence number in a
   DTLS record contained in that packet.

3.2 DCCP and DTLS Connection Handshakes

   Unlike UDP, DCCP is connection-oriented, and has a connection
   handshake procedure that precedes the transmission of DCCP-Data and
   DCCP-DataAck packets. DTLS is also connection-oriented, and has a
   handshake procedure of its own that must precede the transmission of
   actual application information. Using the rule of mapping DTLS
   records to DCCP-Data and DCCP-DataAck packets in section 3, above,
   the two handshakes are forced to happen in series, with the DCCP
   handshake first, followed by the DTLS handshake.

   However, the DCCP handshake packets DCCP-Request and DCCP-Response
   have Application Data fields and can carry user data during the DCCP
   handshake. DTLS implementations MAY choose to transmit the
   ClientHello message in the DCCP-Request packet and the
   HelloVerifyRequest message in the DCCP-Response packet.

   Subsequent DTLS handshake messages, and retransmissions of the
   ClientHello message, if necessary, MUST wait for the completion of
   the DCCP handshake.

3.3 PMTU Discovery

   Each DTLS record must fit within a single DCCP-Data packet. DCCP
   packets are normally transmitted with the DF (Don't Fragment) bit set
   for IPv4, and of course all IPv6 packets are unfragmentable. Because
   of this, DCCP performs Path Maximum Transmission Unit (PMTU)
   Discovery. In determining the maximum size for DTLS records, a DTLS
   over DCCP implementation SHOULD use the DCCP-managed value for PMTU.
   A DTLS over DCCP implementation MAY choose to use its own PMTU
   Discovery calculations, as specified in [RFC4347], but MUST NOT use a
   value greater the value determined by DCCP.

3.4 DCCP Service Codes

   The DCCP connection handshake includes a field called Service Code
   that is intended to describe "the application-level service to which
   the client application wants to connect". Further, "Service Codes
   are intended to provide information about which application protocol
   a connection intends to use, thus aiding middleboxes and reducing
   reliance on globally well-known ports" [RFC4340]. Further rules and
   clarifications for the use of Service Codes are included in [SCODES].

   It is expected that many middleboxes will give different privileges
   to applications running DTLS over DCCP versus just DCCP. Therefore,
   applications that use DTLS over DCCP sometimes and just DCCP other
   times MUST register and use different Service Codes for each mode of
   operation. Applications that use both DCCP and DTLS over DCCP MAY
   choose to listen for incoming connections on the same DCCP port and
   distinguish the mode of the request by the offered Service Code, as
   allowed by [SCODES].

3.5 New Versions of DTLS

As DTLS matures, revisions to and updates for [RFC4347] can be
expected. DTLS includes mechanisms for identifying the version in
use and presumably future versions will either include backward
compatibility modes or at least not allow connections between
dissimilar versions. Since DTLS over DCCP simply encapsulates the
DTLS records transparently, these changes should not affect this
document and the methods of this document should apply to future
versions of DTLS.

Therefore, in the absence of a revision to this document, it is
assumed to apply to all future versions of DTLS. This document will
only be revised if a revision to DTLS makes a revision to the
encapsulation necessary.

It is RECOMMENDED that an application migrating to a new version of
DTLS keep the same DCCP Service Code used for the old version and
allow DTLS to provide the version negotiation support. If the
application developers feel that the new version of DTLS provides
significant new capabilities to the application that will change the
behavior of middleboxes, they MAY use a new Service Code.

4. Security Considerations

Security considerations for DTLS are specified in [RFC4347] and for
DCCP in [RFC4340]. The combination of DTLS and DCCP introduces no
new security considerations.

5. IANA Considerations

There are no IANA actions required for this document.

6. References

6.1 Normative References

[RFC4347]   Rescorla, E., "Datagram Transport Layer Security", RFC
             4347, April 2006.

[RFC4340]   Kohler, E., Handley, M., Floyd, S., "Datagram Congestion
             Control Protocol (DCCP)", RFC 4340, March 2006.

[RFC4346]   Dierks, T. and E. Rescorla, "The Transport Layer Security
             (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
             Requirement Levels", RFC 2119, March 1997.

   [SCODES]   Fairhurst, G., "The DCCP Service Code", draft-ietf-dccp-
                serv-codes-03.txt, June 2007

7. Author's Address

   Tom Phelan
   Sonus Networks
   7 Technology Park Dr.
   Westford, MA USA 01886
   Phone: 978-614-8456
   Email: tphelan@sonusnet.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment