DTLS over DCCP
Internet Draft **T. Phelan**
Document: draft-ietf-dccp-dtls-00.txt **Sonus Networks**
Expires: November 2007 May 2007
Intended status: Proposed Standard

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

Status of this Memo

Abstract

This document describes the use of Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP).

Table of Contents

1. Introduction

This document describes how to use Datagram Transport Layer Security (DTLS), as defined in [RFC4347], over the Datagram Congestion Control Protocol (DCCP), as defined 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 described 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-Data 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 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 above of mapping DTLS records to DCCP-Data packets, the two handshakes must 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 DCCP-Request packets and the HelloVerifyRequest message DCCP-Response packets.

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 described 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]. 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.

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.

4. Security Considerations

Security considerations for DTLS are described 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. 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.

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

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