Network Working Group	C. Jennings
Internet-Draft	Cisco Systems
Intended status: Standards Track	N. Modadugu
Expires: April 12, 2008	Google, Inc.
	October 10, 2007

Session Initiation Protocol (SIP) over Datagram Transport Layer Security (DTLS)
draft-jennings-sip-dtls-05

Status of this Memo

Abstract

This specification defines how to use Datagram Transport Layer Security (DTLS) as a transport for Session Initiation Protocol (SIP). DTLS is a protocol for providing Transport Layer Security (TLS) security over a datagram protocol. This specification also specifies the IANA registrations for using SIP with Datagram Congestion Control Protocol (DCCP). DTLS can be used with either UDP or the Datagram Congestion Control Protocol (DCCP). To accommodate this, this specification also defines how to use SIP directly over DCCP.

---

1. Introduction

Datagram Transport Layer Security (DTLS) (Rescorla, E. and N. Modadugu, “Datagram Transport Layer Security,” April 2006.) [2] provides communication privacy similar to TLS (Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.1,” April 2006.) [9] for datagram packets. SIP can run over both stream and datagram transports, including UDP and TCP. SIP [4] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” June 2002.) already defines how to use TLS with stream oriented transports. This specification extends SIP to use DTLS with datagram oriented transports. Since DTLS can be used with either UDP or the Datagram Congestion Control Protocol (DCCP) as the underlying transport this specification also defines the usage of SIP directly over DCCP.

---

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 RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [5].

---

3. VIA Codes

Via header fields in SIP carry a transport protocol identifier. This specification extends RFC 3261 to define the value "DTLS-UDP" for DTLS over UDP[2] (Rescorla, E. and N. Modadugu, “Datagram Transport Layer Security,” April 2006.) and "DTLS-DCCP" for DTLS over DCCP[1] (Phelan, T., “Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP),” .) and "DCCP" for directly over DCCP[8] (Kohler, E., Handley, M., and S. Floyd, “Datagram Congestion Control Protocol (DCCP),” March 2006.). The update to the ABNF[3] (Crocker, D. and P. Overell, “Augmented BNF for Syntax Specifications: ABNF,” October 2005.) in RFC 3261 for this parameter is the following:

```
transport          =/ "DCCP" / "DTLS-DCCP" / "DTLS-UDP"
```

The following is an example Via header field:

```
Via: SIP/2.0/DTLS-UDP atlanta.example.com:5060
```

4. DTLS and DCCP Usage

The normal rules for sending a request over UDP in RFC 3261 apply to sending over DTLS and directly over DCCP. Note that the congestion safety rules for UDP do not apply to DTLS over DCCP and DCCP. In addition, the normal rules for validating a TLS connection in RFC 3261 apply to DTLS connections. Requests with a SIPS URI can be sent over DTLS as well as TLS.
Note that DCCP performs Path Maximum Transfer Unit (PMTU) discovery. Implementations of SIP over DTLS over DCCP and SIP over DCCP MUST use the PMTU discovered by DCCP when determining the maximum request size for the connection.

4.1. DCCP Option Usage

The following considerations regarding the usage of DCCP options and features apply to the DCCP connections for DTLS and SIP directly over DCCP:

*Congestion Control ID (CCID) negotiation for both directions of the connection MUST include CCID 2 (TCP-like congestion control). CCID 2 optimizes for throughput over smooth rate changes and should be suitable for SIP applications. Applications MAY choose to include other CCIDs, in any preference order.

*Connections MUST NOT use the Minimum Checksum Coverage Feature.

5. Locating DTLS SIP Servers

The normal rules from RFC 3263 (Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” June 2002.) [6] apply when locating a SIP server that supports DTLS. The following new NAPTR[7] (Mealling, M., “Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database,” October 2002.) service values are defined: "SIPS+D2U" for UDP, and "SIPS+D2D" for DCCP[8] (Kohler, E., Handley, M., and S. Floyd, “Datagram Congestion Control Protocol (DCCP),” March 2006.). In addition, the service value "SIP+D2D" should be used for SIP without DTLS directly over DCCP.
The default port for DTLS over UDP or DCCP is 5061. The default port for SIP directly over DCCP is 5060.

6. Security Considerations

The security issues with SIP using DTLS are equivalent to the issues of using SIP with TLS. All the security considerations in RFC 3261 relevant to TLS apply to DTLS.
SIP over DCCP presents the same security issues as SIP over UDP, with the exception that DCCP enforces congestion control at the transport layer.

7. IANA Considerations

This document defines new NAPTR service field values for DTLS over DCCP and UDP as well as over DCCP with no DTLS. IANA is requested to register these values under the "Registry for the SIP SRV Resource Record Services Field". The resulting entries should be:

Services Field	Protocol	Reference
SIPS+D2U	UDP	[RFCXXXX]
SIPS+D2D	DCCP	[RFCXXXX]
SIP+D2D	DCCP	[RFCXXXX]

[Note to RFC Editor: Please replace XXXX with the RFC number of this specification.]
This document registers two new DCCP Service Codes registry as defined by RFC 4340.

Service Code	ASCII	Description	Reference
1936289824	sip	SIP over DCCP	[RFCXXXX]
1936289907	sips	SIP over DCCP over DTLS	[RFCXXXX]

This document defines to new ports in the DCCP Port Numbers Registry as defined by RFC 4340.

Port Name	Port Number	Description	Reference
sip-dccp	5060/dccp	SIP over DCCP	[RFCXXXX]
sip-dtls-dccp	5061/dccp	SIP over DTLS over DCCP	[RFCXXXX]

8. Acknowledgments

Much of text and outline for this specification came from RFC 4168 authored by Jonathan Rosenberg, Henning Schulzrinne, and Gonzalo Camarillo. Jakob Schlyter caught several typos. Eric Rescorla provided helpful comments and text. Tom Phelan provided much of the DCCP text. Thanks also to Colin Perkins.

---

9. References

9.1. Normative References

[1]	Phelan, T., “Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP),” draft-ietf-dccp-dtls (work in progress) (TXT).
[2]	Rescorla, E. and N. Modadugu, “Datagram Transport Layer Security,” RFC 4347, April 2006 (TXT).
[3]	Crocker, D. and P. Overell, “Augmented BNF for Syntax Specifications: ABNF,” RFC 4234, October 2005 (TXT).
[4]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” RFC 3261, June 2002 (TXT).
[5]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (HTML, XML).
[6]	Rosenberg, J. and H. Schulzrinne, “Session Initiation Protocol (SIP): Locating SIP Servers,” RFC 3263, June 2002 (TXT).
[7]	Mealling, M., “Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database,” RFC 3403, October 2002 (TXT).
[8]	Kohler, E., Handley, M., and S. Floyd, “Datagram Congestion Control Protocol (DCCP),” RFC 4340, March 2006 (TXT).

9.2. Informative References

[9]	Dierks, T. and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.1,” RFC 4346, April 2006 (TXT).

Authors' Addresses

	Cullen Jennings

	Cisco Systems
	170 West Tasman Drive
	MS: SJC-21/2
	San Jose, CA 95134
	USA
Phone:	+1 408 902-3341
Email:	fluffy@cisco.com
	Nagendra Modadugu
	Google, Inc.
	1600 Ampitheatre Parkway
	Muntain View, CA 94043
	USA
Email:	ngm@google.com

Full Copyright Statement

Intellectual Property

that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.