Workgroup: NETCONF
Internet-Draft:
draft-unyte-netconf-udp-notif-dtls-00
Published: 30 July 2021
Intended Status: Standards Track
Expires: 31 January 2022
Authors: A. Huang Feng INSA-Lyon
P. Francois INSA-Lyon
T. Zhou Huawei
M. Tollini Swisscom

DTLS for UDP-notif

Abstract

This document describes a DTLS layer for the UDP-notif protocol. DTLS allows a server and a client to exchange secured messages over UDP. This transport layer permits networking devices to send secured UDP-notif messages over the network.

Requirements Language

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 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 31 January 2022.

Copyright Notice

Table of Contents

1. Introduction

UDP-notif [I-D.ietf-netconf-udp-notif] defines a lightweight notification protocol allowing networking devices to send data over UDP. This document describes a layer to secure UDP-notif messages between the publisher and the receiver using the DTLS 1.3 protocol.

The DTLS 1.3 protocol [I-D.draft-ietf-tls-dtls13] is designed to meet the requirements of applications that need to secure datagram transport.

DTLS can be used as a secure transport to counter all the primary threats to UDP-notif:

- *Confidentiality to counter disclosure of the message contents.
- *Integrity checking to counter modifications to a message on a hop-by-hop basis.
- *Server or mutual authentication to counter masquerade.

In addition, DTLS also provides:

- *A cookie exchange mechanism during handshake to counter Denial of Service attacks.
- *A sequence number in the header to counter replay attacks.

This document defines the requirements for the implementation of the secured layer of DTLS for UDP-notif. No DTLS 1.3 extensions are defined nor needed.

Section 2 describes the involved layers for this mechanism. Section 3 describes the port management. Section 4 details the session lifecycle of DTLS within UDP-notif.

2. Transport

As shown in Figure 1, the DTLS is layered next to the UDP transport providing reusable security and authentication functions over UDP. No DTLS extension is required to enable UDP-notif messages over DTLS.

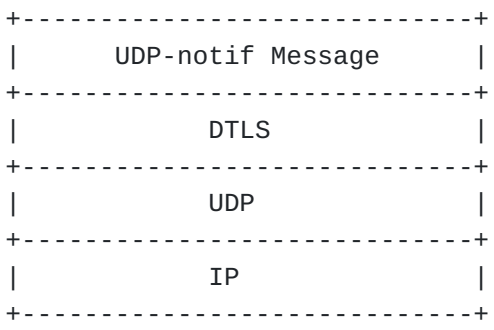

Figure 1: Protocol Stack for DTLS secured UDP-notif

The application implementer will map a unique combination of the remote address, remote port number, local address, and local port number to a session.

Each UDP-notif message is delivered by the DTLS record protocol, which assigns a sequence number to each DTLS record. Although the DTLS implementer may adopt a queue mechanism to resolve reordering, it may not assure that all the messages are delivered in order when mapping on the UDP transport.

Since UDP is an unreliable transport, with DTLS, an originator or a relay may not realize that a collector has gone down or lost its DTLS connection state, so messages may be lost.

The DTLS record has its own sequence number, encryption and decryption will be done by the DTLS layer, so that the UDP-notif Message layer is not impacted by the use of DTLS.

3. Port Assignment

The Publisher is always a DTLS client, and the Receiver is always a DTLS server. The Receivers MUST support accepting UDP-notif Messages

on the specified UDP port, but MAY be configurable to listen on a different port. The Publisher MUST support sending UDP-notif messages to the specified UDP port, but MAY be configurable to send messages to a different port. The Publisher MAY use any source UDP port for transmitting messages.

4. Session lifecycle

4.1. DTLS Session Initiation

The Publisher initiates a DTLS connection by sending a DTLS ClientHello to the Receiver. Implementations MAY support the denial of service countermeasures defined by DTLS 1.3. When these countermeasures are used, the Receiver responds with a DTLS HelloRetryRequest containing a stateless cookie. The Publisher MUST send a new DTLS ClientHello message containing the received cookie, which initiates the DTLS handshake.

The Publisher MUST NOT send any UDP-notif messages before the DTLS handshake has successfully completed.

Implementations MUST support DTLS 1.3 [I-D.draft-ietf-tls-dtls13] and MUST support the mandatory to implement cipher suite TLS_AES_128_GCM_SHA256 and SHOULD implement TLS_AES_256_GCM_SHA384 and TLS_CHACHA20_POLY1305_SHA256 cipher suites, as specified in TLS 1.3 [RFC8446]. If additional cipher suites are supported, then implementations MUST NOT negotiate a cipher suite that employs NULL integrity or authentication algorithms.

Where privacy is REQUIRED, then implementations must either negotiate a cipher suite that employs a non-NULL encryption algorithm or otherwise achieve privacy by other means, such as a physically secured network.

4.2. Publish Data

All UDP-notif messages MUST be published as DTLS "application_data". It is possible that multiple UDP-notif messages are contained in one DTLS record, or that a publication message is transferred in multiple DTLS records. The application data is defined with the following ABNF [RFC5234] expression:

```
APPLICATION-DATA = 1*UDP-NOTIF-FRAME

UDP-NOTIF-FRAME = MSG-LEN SP UDP-NOTIF-MSG

MSG-LEN = NONZERO-DIGIT *DIGIT

SP = %d32
```

NONZERO-DIGIT = %d49-57

DIGIT = %d48 / NONZERO-DIGIT

UDP-NOTIF-MSG is defined in [I-D.ietf-netconf-udp-notif].

The Publisher SHOULD attempt to avoid IP fragmentation by using the Segmentation Option in the UDP-notif message.

4.3. Session termination

A Publisher MUST close the associated DTLS connection if the connection is not expected to deliver any UDP-notif Messages later. It MUST send a DTLS close_notify alert before closing the connection. A Publisher (DTLS client) MAY choose to not wait for the Receiver's close_notify alert and simply close the DTLS connection. Once the Receiver gets a close_notify from the Publisher, it MUST reply with a close_notify.

When no data is received from a DTLS connection for a long time, the Receiver MAY close the connection. Implementations SHOULD set the timeout value to 10 minutes but application specific profiles MAY recommend shorter or longer values. The Receiver (DTLS server) MUST attempt to initiate an exchange of close_notify alerts with the Publisher before closing the connection. Receivers that are unprepared to receive any more data MAY close the connection after sending the close_notify alert.

Although closure alerts are a component of TLS and so of DTLS, they, like all alerts, are not retransmitted by DTLS and so may be lost over an unreliable network.

5. IANA Considerations

This RFC requests that IANA assigns one UDP port number in the "Registered Port Numbers" range with the service name "udp-notif-dtls". This port will be the default port for the UDP-based notification Streaming Telemetry (UDP-Notif-DTLS) for NETCONF and RESTCONF. Below is the registration template following the rules of [RFC6335].

Service Name: udp-notif-dtls

Transport Protocol(s): UDP

Assignee: IESG <iesg@ietf.org>

Contact: IETF Chair <chair@ietf.org>

Description: UDP-based Publication Streaming Telemetry

Reference: [RFC-to-be]

Port Number: TBD1

IANA is requested to assign a new URI from the IETF XML Registry [RFC3688]. The following URI is suggested:

```
URI: urn:ietf:params:xml:ns:yang:ietf-udp-notif
Registrant Contact: The IESG.
XML: N/A; the requested URI is an XML namespace.
```

This document also requests a new YANG module name in the YANG Module Names registry [RFC7950] with the following suggestion:

```
name: ietf-udp-notif
namespace: urn:ietf:params:xml:ns:yang:ietf-udp-notif-dtls
prefix: un
reference: RFC XXXX
```

6. References

6.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <https://www.rfc-editor.org/info/rfc3688>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[RFC6335] Cotton, M., Eggert, L., Touch, J., Westerlund, M., and S. Cheshire, "Internet Assigned Numbers Authority (IANA) Procedures for the Management of the Service Name and Transport Protocol Port Number Registry", BCP 165, RFC

6335, DOI 10.17487/RFC6335, August 2011, <https://www.rfc-editor.org/info/rfc6335>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

6.2. Informative References

[I-D.draft-ietf-tls-dtls13] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13-43, July 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-dtls13-43>.

[I-D.ietf-netconf-udp-notif] Zheng, G., Zhou, T., Graf, T., Francois, P., and P. Lucente, "UDP-based Transport for Configured Subscriptions", Work in Progress, Internet-Draft, draft-ietf-netconf-udp-notif-03, July 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-netconf-udp-notif-03>.

Authors' Addresses

Alex Huang Feng
INSA-Lyon
Lyon
France

Email: alex.huang-feng@insa-lyon.fr

Pierre Francois
INSA-Lyon
Lyon
France

Email: pierre.francois@insa-lyon.fr

Tianran Zhou
Huawei
156 Beiqing Rd., Haidian District
Beijing
China

Email: zhoutianran@huawei.com

Marco Tollini
Swisscom
Binzring 17
CH- Zuerich 8045
Switzerland

Email: marco.tollini1@swisscom.com