         Additional Considerations for UDP Encapsulation of Stream Control
                    Transmission Protocol (SCTP) Packets
                 draft-tuexen-tsvwg-sctp-udp-encaps-cons-09

Abstract

   RFC 6951 specifies the UDP encapsulation of SCTP packets. The
   described handling of received packets requires the check of the
   verification tag. However, RFC 6951 misses a specification of the
   handling of received packets for which this check is not possible.

   This document updates RFC 6951 by specifying the handling of received
   packets for which the verification tag can not be checked.

Table of Contents

1. Introduction

   [RFC6951] specifies the UDP encapsulation of SCTP packets. To be
   able to adopt automatically to changes of the remote UDP
   encapsulation port number, it is updated when processing received
   packets. This includes automatic enabling and disabling of UDP
   encapsulation.

   Section 5.4 of [RFC6951] describes the processing of received packets
   and requires the check of the verification tag before updating the
   remote UDP encapsulation port and the possible enabling or disabling
   of UDP encapsulation.

   [RFC6951] basically misses a description of the handling of received
   packets where checking the verification tag is not possible. This
   includes packets for which no association can be found and packets
   containing an INIT chunk, since the verification tag of these packets
   is 0.

2. Conventions

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
   "OPTIONAL" in this document are to be interpreted as described in BCP
   14 [RFC2119] [RFC8174] when, and only when, they appear in all
   capitals, as shown here.

3. Handling of Out of the Blue Packets

    If the processing of an out of the blue packet requires the sending
    of a packet in response according to the rules specified in
    Section 8.4 of [RFC9260], the following rules apply:

    1. If the received packet was encapsulated in UDP, the response
        packets MUST also be encapsulated in UDP. The UDP source port
        and UDP destination port used for sending the response packet are
        the UDP destination port and UDP source port of the received
        packet.

    2. If the received packet was not encapsulated in UDP, the response
        packet MUST NOT be encapsulated in UDP.

    Please note that in these cases a check of the verification tag is
    not possible.

4. Handling of SCTP Packets Containing an INIT Chunk Matching an
    Existing Associations

    SCTP packets containing an INIT chunk have the verification tag 0 in
    the common header. Therefore the verification tag can't be checked.

    The following rules apply when processing the received packet:

    1. The remote UDP encapsulation port for the source address of the
        received SCTP packet MUST NOT be updated if the encapsulation of
        outgoing packets is enabled and the received SCTP packet is
        encapsulated.

    2. The UDP encapsulation for outgoing packets towards the source
        address of the received SCTP packet MUST NOT be enabled, if it is
        disabled and the received SCTP packet is encapsulated.

    3. The UDP encapsulation for outgoing packets towards the source
        address of the received SCTP packet MUST NOT be disabled, if it
        is enabled and the received SCTP packet is not encapsulated.

4. If the UDP encapsulation for outgoing packets towards the source address of the received SCTP packet is disabled and the received SCTP packet is encapsulated, an SCTP packet containing an ABORT chunk MUST be sent. The ABORT chunk MAY include the error cause defined below indicating an "Restart of an Association with New Encapsulation Port". This packet containing the ABORT chunk MUST be encapsulated in UDP. The UDP source port and UDP destination port used for sending the packet containing the ABORT chunk are the UDP destination port and UDP source port of the received packet containing the INIT chunk.

5. If the UDP encapsulation for outgoing packets towards the source address of the received SCTP packet is disabled and the received SCTP packet is not encapsulated, the processing defined in [RFC9260] MUST be performed. If a packet is sent in response, it MUST NOT be encapsulated.

6. If the UDP encapsulation for outgoing packets towards the source address of the received SCTP packet is enabled and the received SCTP packet is not encapsulated, an SCTP packet containing an ABORT chunk MUST be sent. The ABORT chunk MAY include the error cause defined below indicating an "Restart of an Association with New Encapsulation Port". This packet containing the ABORT chunk MUST NOT be encapsulated in UDP.

7. If the UDP encapsulation for outgoing packets towards the source address of the received SCTP packet is enabled and the received SCTP packet is encapsulated, but the UDP source port of the received SCTP packet is not equal to the remote UDP encapsulation port for the source address of the received SCTP packet, an SCTP packet containing an ABORT chunk MUST be sent. The ABORT chunk MAY include the error cause defined below indicating an "Restart of an Association with New Encapsulation Port". This packet containing the ABORT chunk MUST be encapsulated in UDP. The UDP source port and UDP destination port used for sending the packet containing the ABORT chunk are the UDP destination port and UDP source port of the received packet containing the INIT chunk.

8. If the UDP encapsulation for outgoing packets towards the source address of the received SCTP packet is enabled and the received SCTP packet is encapsulated and the UDP source port of the received SCTP packet is equal to the remote UDP encapsulation port for the source address of the received SCTP packet, the processing defined in [RFC9260] MUST be performed. If a packet is sent in response, it MUST be encapsulated. The UDP source port and UDP destination port used for sending the packet containing the ABORT chunk are the UDP destination port and UDP source port of the received packet containing the INIT chunk.

The error cause indicating an "Restart of an Association with New
Encapsulation Port" is defined by the following figure.

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Cause Code = 14 (suggested)   |      Cause Length = 8         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Current Encapsulation Port    |    New Encapsulation Port    |
+----------------------------------+----------------------------+
```

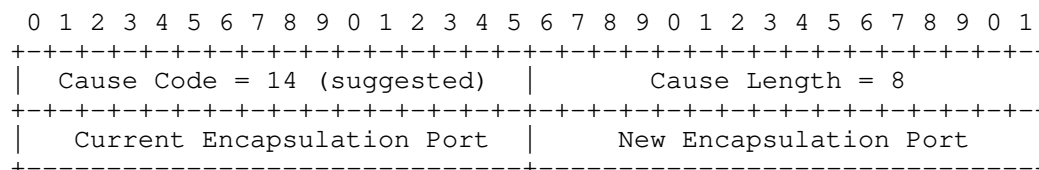   Figure 1: Restart of an Association with New Encapsulation Port
                              Error Cause

Cause Code: 2 bytes (unsigned integer)
   This field holds the IANA defined cause code for the "Restart of
   an Association with New Encapsulation Port" error cause. IANA is
   requested to assign the value 14 (suggested) for this cause code.

Cause Length: 2 bytes (unsigned integer)
   This field holds the length in bytes of the error cause; the value
   MUST be 8.

Current Encapsulation Port: 2 bytes (unsigned integer)
   This field holds the remote encapsulation port currently being
   used for the destination address the received packet containing
   the INIT chunk was sent from. If the UDP encapsulation for
   destination address is currently disabled, 0 is used.

New Encapsulation Port: 2 bytes (unsigned integer)
   If the received SCTP packet containing the INIT chunk is
   encapsulated in UDP, this field holds the UDP source port number
   of the UDP packet. If the received SCTP packet is not
   encapsulated in UDP, this field is 0.

All transported integer numbers are in "network byte order" a.k.a.,
Big Endian.

5. Middlebox Considerations

   Middleboxes often use different timeouts for UDP based flows than for
   other flows. Therefore the HEARTBEAT.Interval parameter SHOULD be
   lowered to 15 seconds when UDP encapsulation is used.

6. IANA Considerations

   [NOTE to RFC-Editor: "RFCXXXX" is to be replaced by the RFC number
   you assign this document.]

[NOTE to RFC-Editor: The requested values for the cause code are
tentative and to be confirmed by IANA.]

This document (RFCXXXX) is the reference for the registration
described in this section.

A new error cause code has to be assigned by IANA. This requires an
additional line in the "Error Cause Codes" registry for SCTP:

Value	Cause Code	Reference
================	===============================	===========
14 (suggested)	Restart of an Association with New Encapsulation Port	[RFCXXXX]

Table 1: New entry in Error Cause Codes registry

7. Security Considerations

This document does not change the considerations given in [RFC6951].

However, not following the procedures given in this document might
allow an attacker to take over SCTP associations. The attacker needs
only to share the IP address of an existing SCTP association.

If firewalls will be applied at the SCTP association level, they have
to take the UDP encapsulation into account.

8. 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>.

[RFC6951] Tuexen, M. and R. Stewart, "UDP Encapsulation of Stream
           Control Transmission Protocol (SCTP) Packets for End-Host
           to End-Host Communication", RFC 6951,
           DOI 10.17487/RFC6951, May 2013,
           <https://www.rfc-editor.org/info/rfc6951>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
           2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
           May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC9260]   Stewart, R., Tüxen, M., and K. Nielsen, "Stream Control
               Transmission Protocol", RFC 9260, DOI 10.17487/RFC9260,
               June 2022, <https://www.rfc-editor.org/info/rfc9260>.

Acknowledgments

Authors' Addresses

   Michael Tüxen
   Münster University of Applied Sciences
   Stegerwaldstrasse 39
   48565 Steinfurt
   Germany
   Email: tuexen@fh-muenster.de

   Randall R. Stewart
   15214 Pendio Drive
   Bella Collina, FL 34756
   United States of America
   Email: randall@lakerest.net