

SCTP

STATEMENT OF COMPLIANCE

STATEMENT OF COMPLIANCE

Copyright

© Ericsson AB 2013-2014. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.



Contents

1	General	1
1.1	Introduction	1
1.2	Terms	1
1.3	Concept	1
2	Compliance Lists	3
2.1	IETF - Stream Control Transmission Protocol	3
3	Notes	5
	Reference List	7



SCTP



1 General

1.1 Introduction

This document describes to what extent the Ericsson SCTP signaling component conforms with the IETF RFC 5062 (see Reference [1]).

1.2 Terms

ICMP	Internet Control Message Protocol
IP	Internet Protocol
RFC	Request For Comments
SCTP	Stream Control Transmission Protocol

1.3 Concept

The terms that are used are:

C	The Ericsson signaling component complies with the specified section in RFC 5062 (see Reference [1]).
N	The Ericsson signaling component does not comply with the specified section in RFC 5062 (see Reference [1]).
P	The Ericsson signaling component complies partly with the specified section in RFC 5062 (see Reference [1]).
-	There is nothing to implement in the referred section (always placed in column C).





2 Compliance Lists

2.1 IETF - Stream Control Transmission Protocol

2.1.1 RFC 5062

Table 1 RFC 5062

Reference		C	N	P	Comments
1	Introduction	-			
2	Address Camping or Stealing			X	Note 1 Note 2
3	Association Hijacking 1	X			Note 3
4	Association Hijacking 2	X			Note 4
5	Bombing Attack (Amplification) 1	X			Note 5
6	Bombing Attack (Amplification) 2	X			Note 6
7	Association Redirection	X			Note 7
8	Bombing Attack (Amplification) 3	X			Note 8
9	Bombing Attack (Amplification) 4	X			Note 9 Note 10
10	Bombing Attack (Amplification) 5	X			Note 8
11	Security Considerations	-			
References		-			





3 Notes

- Note 1** BASE SCTP supports Initial Path Probing which partly replaces Path Verification mechanism described in **Reference [2]**. Initial Path Probing mitigate the concerned attack. More information about Initial Path Probing could be found in **Reference [4]**.
- Note 2** BASE SCTP does not choose port numbers on a random basis if the port numbers are not specified. Instead BASE SCTP has its own algorithm for port assignment. The algorithm uses some variables which are unknown outside the stack. This makes it hard for an attacker to guess the port number. More information about the algorithm could be found in **Reference [4]**.
- Note 3** BASE SCTP does not support RFC 5061 therefore it is not vulnerable to the concerned attack.
- Note 4** Concerned attack is not based on a weakness of the SCTP protocol, but on the ignorance of the upper layer. SCTP cannot mitigate it itself.
- Note 5** BASE SCTP supports ICMP handling, Initial Path Probing and aborts the association if it receives a SACK acknowledging a TSN that has not been sent. All these mechanisms mitigate the concerned attack.
- Note 6** BASE SCTP supports “HB.Max.Burst” configuration parameter and the recommended value is 1. Moreover BASE SCTP supports “Allowed Increment Cookie Life” configuration parameter which limits increasing of cookie lifetime and the recommended value for this parameter is 0 (no increase). The concerned attack can be mitigated by means of configuring “HB.Max.Burst” properly. See **Reference [3]** for more information about the mentioned configuration parameters.
- Note 7** BASE SCTP stores port numbers in COOKIE and does not accept the association if the port numbers have been modified.
- Note 8** BASE SCTP is able to bundle several control chunks, which acknowledges some incoming chunks, into a single IP packet.

**Note 9**

BASE SCTP limits the size of INIT ACK chunk by the “Size of outgoing IP buffer” configuration parameter. If this limit is reached, SCTP does not send INIT ACK chunk and reports an error. See **Reference [3]** for more information about the mentioned configuration parameter.

Note10

BASE SCTP silently discards PAD chunks including the case when they are bundled with INIT chunk. Thus, incoming INIT with bundled PAD chunks will not result in sending of big INIT ACK in response.



Reference List

IETF

- [1] *R. Stewart, "Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures", RFC 5062. September 2007.*
- [2] *R. Stewart, "Stream Control Transmission Protocol", RFC 4960. Standards Track. September 2007.*
- [3] *Configuration File Description for SCTP IETF 19073-CAA 901 548 Uen*
- [4] *Functional Specification for SCTP IETF 155 17-CAA 901 548 Uen*