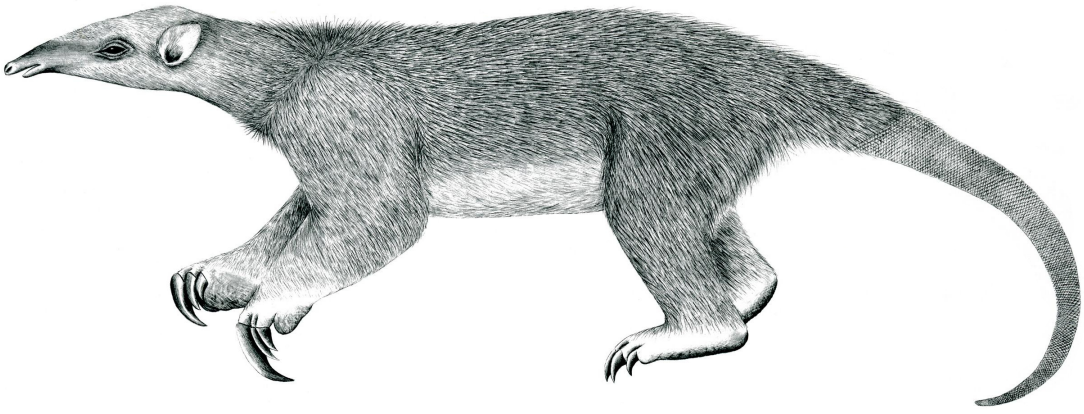
Tranalyzer2

sctpDecode

Stream Control Transmission Protocol (SCTP)



Tranalyzer Development Team

Contents

1 sctpDecode

1.1 Description

The sctpDecode plugin produces a flow based view of SCTP operations between computers for anomaly detection and troubleshooting purposes.

1.2 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
SCTP_CRCADL32CHK	0	Checksum computation: 0: No checksum computation 1: CRC32 2: ADLER32	
SCTP_CHNKVAL	0	Chunk type representation: 0: chunk type bit field 1: chunk type value 2: chunk type as string	
SCTP_CHNKAGGR	0	Aggregate chunk types	SCTP_CHNKVAL>0
SCTP_TSNREL	0	1: Relative TSN, 0: Absolute TSN	
SCTP_MAXCTYPE	15	Maximum chunk types to store/flow	SCTP_CHNKVAL>0
SCTP_ASMX	10	Maximum ASCONF IP	
SCTP_MXADDR	5	Maximum number of addresses to print in packet mode	

1.3 Flow File Output

The sctpDecode plugin outputs the following columns:

Column	Type	Description	Flags
sctpStat	H8	Status	
sctpDSNum	U16	Data stream number	SCTP_ACTIVATE=1
sctpMaxDSNum	U16	Max. number of data streams	SCTP_ACTIVATE=0
sctpPID	U32	Payload ID	
sctpVTag	H32	Verification tag	
sctpTypeBF	H16	Aggregated type bit field	SCTP_CHNKVAL=0
sctpType	R(U8)	Unique types values	SCTP_CHNKVAL=1
sctpTypeN	R(SC)	Unique types names	SCTP_CHNKVAL=2
sctpCntD_I_A	U16_U16_U16	DATA, INIT and ABORT count	
sctpCFlags	H8	Aggregated chunk flag	
sctpCCBF	H16	Aggregated error cause code bit field	
sctpASIP4	R(SC)	ASCONF IPv4	
sctpASIP6	R(SC)	ASCONF IPv6	
sctpIS	U16	Inbound streams	
sctpOS	U16	Outbound streams	
sctpIARW	U32	Initial Advertised Receiver Window	

Column	Type	Description Flags
sctpIARWMin	U32	Initial Advertised Receiver Window Minimum
sctpIARWMax	U32	Initial Advertised Receiver Window Maximum
sctpARW	F	Advertised Receiver Window

1.3.1 sctpStat

The `sctpStat` column is to be interpreted as follows:

	sctpStat	Description
2^0	(=0x01)	Adler32 error
2^1	(=0x02)	CRC32 error
2^2	(=0x04)	Chunk padded
2^3	(=0x08)	Chunk truncated
2^6	(=0x10)	3 ACK
2^7	(=0x20)	Type Field overflow
2^4	(=0x40)	Do not report
2^5	(=0x80)	Stop processing of the packet

1.3.2 sctpTypeN, sctpTypeBF and sctpType

The `sctpTypeN`, `sctpTypeBF` and `sctpType` columns are to be interpreted as follows:

sctpTypeN	sctpTypeBF	sctpType	Description
0	0x0001	DATA	Payload data
1	0x0002	INIT	Initiation
2	0x0004	INIT_ACK	Initiation acknowledgement
3	0x0008	SACK	Selective acknowledgement
4	0x0010	HEARTBEAT	Heartbeat request
5	0x0020	HEARTBEAT_ACK	Heartbeat acknowledgement
6	0x0040	ABORT	Abort
7	0x0080	SHUTDOWN	Shutdown
8	0x0100	SHUTDOWN_ACK	Shutdown acknowledgement
9	0x0200	ERROR	Operation error
10	0x0400	COOKIE_ECHO	State cookie
11	0x0800	COOKIE_ACK	Cookie acknowledgement
12	0x1000	ECNE	Explicit congestion notification echo (reserved)
13	0x2000	CWR	Congestion window reduced (reserved)
14	0x4000	SHUTDOWN_COMPLETE	Shutdown complete
15	0x8000	AUTH	Authentication chunk

1.3.3 sctpCFlags

The `sctpCFlags` column is to be interpreted as follows:

sctpCFlags	Description
2^0 (=0x01)	Last segment
2^1 (=0x02)	First segment
2^2 (=0x04)	Ordered delivery
2^3 (=0x08)	Possibly delay SACK
2^4 (=0x10)	—
2^5 (=0x20)	—
2^6 (=0x40)	Transmission sequence number error
2^7 (=0x80)	Association sequence number error

1.3.4 sctpCCBF

The sctpCCBF column is to be interpreted as follows:

sctpCCBF	Description
2^0 (=0x0001)	—
2^1 (=0x0002)	Invalid Stream Identifier
2^2 (=0x0004)	Missing Mandatory Parameter
2^3 (=0x0008)	Stale Cookie Error
2^4 (=0x0010)	Out of Resource
2^5 (=0x0020)	Unresolvable Address
2^6 (=0x0040)	Unrecognized Chunk Type
2^7 (=0x0080)	Invalid Mandatory Parameter
2^8 (=0x0100)	Unrecognized Parameters
2^9 (=0x0200)	No User Data
2^{10} (=0x0400)	Cookie Received While Shutting Down
2^{11} (=0x0800)	Restart of an Association with New Addresses
2^{12} (=0x1000)	User Initiated ABORT
2^{13} (=0x2000)	Protocol Violation
2^{14} (=0x4000)	—
2^{15} (=0x8000)	Error code > 14

1.4 Packet File Output

In packet mode (-s option), the sctpDecode plugin outputs the following columns:

Column	Type	Description	Flags
sctpVTag	H32	Verification tag	
sctpChkSum	H32	Checksum	
sctpCalCRCChkSum	H32	Computed CRC checksum	SCTP_CRCADL32CHK=1
sctpCalADLChkSum	H32	Computed ADLER32 checksum	SCTP_CRCADL32CHK=2

Column	Type	Description	Flags
sctpChunkType_	U8_	Chunk type,	
sid_	U16_	stream identifier,	
flags_	H8_	chunk flags,	
numDPkts_	U16_	DATA count,	
len_	I32_	chunk length,	
pid	U32	Payload ID	
sctpNChunks	U8	Number of chunks	
sctpCCBF	H16	Aggregated error cause code bit field	
sctpARW	U32	Advertised Receiver Window	
sctpPID	U32	Payload ID	
sctpStat	U8	Status	
sctpTSN	U32	Transmission Sequence Number (TSN)	SCTP_TSNREL=0
sctpTSNAck	U32	TSN Acknowledgement	SCTP_TSNREL=0
sctpRelTSN	U32	Relative Transmission Sequence Number (TSN)	SCTP_TSNREL=1
sctpRelTSNAck	U32	Relative TSN Acknowledgement	SCTP_TSNREL=1
sctpASIP4	R(IP4)	ASCONF IPv4	
sctpASIP6	R(IP6)	ASCONF IPv6	

1.5 Plugin Report Output

The following information is reported:

- Aggregated sctpStat
- Aggregated sctpCFlags
- Aggregated sctpTypeBF