SCTP and its Support in Wireshark
June 18th, 2009

Michael Tüxen
Professor / Wireshark Core Developer | Münster University of Applied Sciences

SHARKFEST '09
Stanford University
June 15-18, 2009
Outline

• History of SCTP.
• Introduction to SCTP.
• Services provided by SCTP.
• SCTP support in Wireshark.
• Conclusion.
The IP Protocol Suite

DNS  RTP  HTTP  SMTP  FTP  SS7/IP  AAA  IPFIX  RTP

UDP  TCP  SCTP  DCCP

IP Version 4 / IP Version 6
Why was SCTP developed?

• In 1999 the IETF (SIGTRAN working group) started to work on SS7/IP.

• Neither UDP nor TCP provided the necessary network fault tolerance:
  – Head of line blocking when packets are lost.
  – Switch to an alternate path when a path fails.

• So a new transport protocol was developed for SIGTRAN: *Simple Control Transmission Protocol* (SCTP). But the name was changed…
Where is SCTP used?

- Telephony signaling networks, especially UMTS.
- Diameter (successor of Radius).
- IPFIX (successor of NetFlow).
- Ongoing research:
  - MPI
  - HTTP/SCTP
  - Network file systems
  - SSH, DNS
Implementations

- Part of FreeBSD 7.0 and higher.
- Part of all recent 2.6 kernels.
- Part of Solaris 10.
- For FreeBSD, Linux, Solaris, Mac OS X, HP-UX and Windows: sctplib (userland library) available from http://www.sctp.de.
- Several commercial implementations.
Features of SCTP: Base Protocol

- Packet oriented.
- Connection oriented.
- Reliable Transport.
- Flow and congestion control.
- Supports multiple unidirectional streams.
- Supports multihoming (IPv4 and/or IPv6).
- Supports bundling of multiple user messages.
- Fragmentation and reassembly.
Features of SCTP: Protocol Extensions

• User controlled partial reliability.
• Support for SCTP-AUTH.
• Dynamic reconfiguration of addresses during the lifetime of an association.
• Dynamic reconfiguration of Streams.
• Advanced path MTU discovery.
SCTP Terminology

• An SCTP connection is called an association.
• SCTP uses the same port number concept as TCP and UDP do.
• An SCTP endpoint can be identified (at a certain point of time) by a pair of a list of IP-addresses and a port number.
SCTP Message Format

- Common Header
- First Chunk
- Second Chunk
- Third Chunk
- Last Chunk
# SCTP Common Header Format

<table>
<thead>
<tr>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Verification Tag</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Checksum</th>
</tr>
</thead>
</table>
## SCTP Chunk Format

<table>
<thead>
<tr>
<th>Type</th>
<th>Flags</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Value**
- **Padding**
SCTP Chunk Types

- INIT, INIT-ACK, COOKIE-ECHO, COOKIE-ACK.
- DATA, SACK.
- SHUTDOWN, SHUTDOWN-ACK, SHUTDOWN-COMPLETE.
- HEARTBEAT, HEARTBEAT-ACK.
- ERROR, ABORT.
- FORWARD-TSN.
- ASCONF, ASCONF-ACK.
- AUTH.
Association Setup

- Peer to peer model (including client/server).
- Four way handshake is used.
- Important parameters exchanged:
  - Verification tag.
  - Maximum receiver window.
  - Number of streams.
  - IP addresses (IPv4 and/or IPv6).
- Cookie-based mechanism.
The Verification Tag

• 32-bit random number.
• Chosen by each end-point.
• The protection against blind attackers is based on the verification tag.
• Stays the same during the lifetime of an association.
• Some implementations use it for looking up the association.
• If a packet is received with a wrong verification tag it is silently discarded.
Multihoming

• Every IP address of the peer is considered as a path.
• All paths are continuously supervised and initially confirmed.
• One path, the so called primary path, is used for initial data transmission.
• In the case of (timer based) retransmissions an alternate path is used.
• Loadsharing is subject of ongoing research.
Partial In-sequence Delivery

- A lot of applications do not require all data to be delivered in sequence.
- Therefore SCTP supports the streams concept. Only data sent within the same stream is delivered in sequence relative to that stream.
- This minimizes the impact of head of line blocking in case of message loss.
- In addition: Unordered delivery in each stream.
Partial Reliability

• The sender has the capability of notifying the receiver that a particular DATA chunk will never arrive at the receiver.
• PR-SCTP is a general concept.
• Applications:
  – Data may have a limited life time.
  – Data may have one of several priorities and share a resource.
  – Data may only be transmitted a limited number of times.
Dynamic Address Reconfiguration

• Reliable systems must be reconfigured without interruption of the service.
• ADDIP allows to delete and add IP-addresses during the lifetime of an association.
• Security is based on SCTP-AUTH.
• IP-addresses are transported inside ASCONF chunks.
• For example, it supports IPv6 renumbering.
Wireshark Support

- SCTP Base protocol and all extensions (I’m aware of) are supported.
- Configurable via 
  Edit->Preferences->Protocols->SCTP.
- Associations based analysis even if initial handshake is not included in the capture file.
- Graphical analysis.
An Example: basic_sctp.pcap

- Shows
  - the association setup.
  - the association teardown.
  - a simple exchange of user data.
  - a lot of parameters in the INIT and INIT-ACK chunk.
Dissecting Upper Layers

• All SIGTRAN protocols, a lot of SS7 protocols.
• Upper layers are detected by
  – looking at the payload protocol identifier.
  – looking at the smaller port number
  – looking at the larger port number
  – heuristic dissectors (precedence configurable)
• Dissection of upper layers can be switched off.
• Can manually be selected: Analyze->Decode As
Reassembly

- Needs to be enabled in the protocol preferences.
- Is required to dissect upper layer protocols when the user message is fragmented.
- Is demoed by using frag_sctp.pcap.
TSN analysis

- Needs to be enabled in the protocol preferences.
- For a DATA chunk shows in which frame it is acknowledged.
- For a SACK chunk shows which DATA chunk it acknowledges and in which frame they are.
- Show the round trip time (RTT).
- Is demoed using basic_sctp.pcap.
Association analysis

• Much more complex than for UDP or TCP.
• Based on the handshake messages, if available, and makes used of verification tag based heuristics.
• Can be used to analyze the particular association or show all associations.
• Demoed by using multi_sctp.pcap.
Graphical Analysis

• Can draw TSN over time per association including acknowledgements.
• Can draw bytes over time per association.
• You can zoom in.
• Very useful to get an overview.
• Demoed by using data_sctp.pcap.
Capturing on Multiple Interfaces

• Currently only supported by the any interface on Linux platforms.
• Needs multiple instances of dumpcap and post-processing with mergecap.
• An alternative: using a switch with port mirroring.
• ... there is room for improvement.
Conclusion

• SCTP is a very powerful transport protocol available on (almost) all Unix like platforms.
• Wireshark provides excellent support for SCTP.
• Support for capturing on multiple interfaces will be improved...
Questions and/or Suggestions?