Native SCTP, DCCP, UDP-Lite and Home Gateway NATs

Runa Barik (UiO), Michael Welzl, Gorry Fairhurst, Thomas Dreibholz, Ahmed Elmokashfi, Stein Gjessing

maprg @104th IETF Meeting
Prague
28th March 2019
Methodology

- Detecting support for native SCTP, DCCP, UDPLite using transport header checksum (and Vtag for native SCTP).
- Using local testbed to study NAT boxes
  - Off-the-shelf equipment tests
  - `netfilter` in Linux
  - IPF, PF and IPFW in FreeBSD
- Lessons learnt
Off-the-shelf equipment tests

- Dlink: DIR 655-A2, A3, B1; DIR 619-Ax; DI-614+-B2
- Jensen: Air:Link WBR 7954 v2, v3; AirLink 1000Gv2 (A)
- Linksys: E2500, WRT54G/ GL/GS v1.1, WRT54G, E4200
- Netgear: WGR 614v7, WGR 614v9, WNDR3400
- Topcom: WBR 254G, BR 604
- TP-LINK: TL-MR3020 v1, TL-WR703N
- 3G modem: WR3G050-02 (Spi59-YJ v2.0)
- ZyXEL: P8702N, P-2812HNU-F3
- Edimax: BR-6574N (A)
- Xiaomi: Router 3C

OS and versions:

- Linux 2.4-Linux 4.4, ThreadX, VxWorks, OpenWRT MiWiFi ROM, Unknown.
<table>
<thead>
<tr>
<th>Protocol with transport header checksum</th>
<th>Observation</th>
<th>Obs. No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP with zero checksum</td>
<td>NA(P)Ting with zero checksum</td>
<td>Obs-1</td>
</tr>
<tr>
<td>DCCP, SCTP, UDP-Lite and unassigned number</td>
<td>NAT’ing, i.e. no transport header update</td>
<td>Obs-2</td>
</tr>
<tr>
<td>DCCP, SCTP, UDP-Lite and unassigned number</td>
<td>No NAT’ing</td>
<td>Obs-3</td>
</tr>
<tr>
<td>DCCP, SCTP, UDP-Lite and unassigned number</td>
<td>Dropping</td>
<td>Obs-4</td>
</tr>
</tbody>
</table>

**Table:** Behavior of transport protocols across the middleboxes

- UDP with zero checksum remains intact in all devices.
- VxWorks OS follows Obs-4 for new transport protocols.
- Jensen, Topcom and some Dlink devices follow Obs-3.
- The remaining devices follow IP-level NAT’ing (success for SCTP, but not for DCCP and UDPLite).
Netfilter in Linux

- Linux kernel (version 3.18.109 for MIPS architecture) in TP-Link TL-MR3020, using OpenWRT.
- Netfilter: conntrack_proto_X and nat_proto_X
  - \( X = \{\text{SCTP, DCCP, UDPLite}\} \)

**conntrack_proto_X**: Responsible for transport header verification, NATing, state machine. It fails for port collision.

**nat_proto_X**: Responsible for port-mapping and checksum update.

- Linux netfilter supports SCTP, DCCP and UDPLite.
- Netfilter changes the SCTP port on collision.
- `sysctl` variable `nf_contrack_checkum` verifies the checksum on incoming packets
Used FreeBSD 11.2 in a x86-64 PC.
Firewall variants of FreeBSD: IPF, PF and IPFW
No support for DCCP and UDPLite.
Only IPFW/libalias supports SCTP.
### FreeBSD

<table>
<thead>
<tr>
<th>Protocol</th>
<th>IPFW (first / later clients)</th>
<th>PF (first / later clients)</th>
<th>IPF (first / later clients)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP with zero checksum</td>
<td>Obs-1 / Obs-1</td>
<td>Obs-1 / Obs-1</td>
<td>Obs-1 / Obs-1</td>
</tr>
<tr>
<td>DCCP, UDP-Lite</td>
<td>Obs-2 / Obs-2*</td>
<td>Obs-2 / Obs-4</td>
<td>Obs-2 / Obs-3</td>
</tr>
<tr>
<td>SCTP</td>
<td>Obs-2 / Obs-2</td>
<td>Obs-2 / Obs-4</td>
<td>Obs-2 / Obs-3</td>
</tr>
</tbody>
</table>

**Table:** Behavior of transport protocols in FreeBSD NAT firewalls (*: the response packets are forwarded to the last client)

<table>
<thead>
<tr>
<th>Observation</th>
<th>Obs. No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obs-1</td>
<td>NA(P)Ting with zero checksum</td>
</tr>
<tr>
<td>Obs-2</td>
<td>NAT’ing, i.e. no transport header update</td>
</tr>
<tr>
<td>Obs-3</td>
<td>No NAT’ing</td>
</tr>
<tr>
<td>Obs-4</td>
<td>Dropping</td>
</tr>
</tbody>
</table>

**Table:** Behavior of transport protocols across the middleboxes
Idle-timeout of NAT devices

Smaller idle-timeout is good for SCTP.

![Graph showing idle-timeout in seconds]

Idle Timeout (in seconds)
Lessons learnt

- Configurable support in the device setting for checksum verification or new transport protocols.
- Emulating UDP-Lite with UDP with zero checksum.
- Native protocols are not enabled by default.
- An unusual mechanism or a new option in UDP or TCP has greater chances of success than a new protocol.
- Avoiding the pseudo-header for checksum calculation could improve the chances of NAT traversals.
- To support multi-homing feature, individual connections to a NAT should look like single-homed ones.
Q&A?
Sequence diagram showing SCTP multi-homing support