IPv6 DOTS Signal Option

draft-francois-dots-ipv6-signal-option-01

Jérôme François, Inria, jerome.francois@inria.fr
Abdelkader Lahmadi, Université de Lorraine,
abdelkader.lahmadi@loria.fr
Marco Davids, SIDN Labs, marco.davids@sidn.nl
Giovane Moura, SIDN Labs, giovane.moura@sidn.nl

IETF 98 Chicago
Key idea

- Objective: signal DDoS attacks from a DOTS client (detection) to DOTS server (mitigation)
- Regular signalling paths for delivering DOTS signals might be also affected by the DDoS → Adding an auxiliary mechanism for signaling (does not substitute)
- Use IPv6 Hop-by-Hop Option Header [RFC2460]
  - Embed the information into pre-existing packet
  - signaling information is embedded into outgoing IPv6 packets
  - in an opportunistic manner (not all packets, not only those outgoing to the DOTS server... but some well chosen)
  - the DOTS client initiate this process, intermediate capable routers can store the information and embed it into other packets
Option processing

- Selection of packets is rule-based to only consider a subset
- A sequence of rules where each is defined by
  - 1st level: a filter on IPv6 header to be matched
  - 2nd level: a ratio of previously matched packets
  - + a timeout
- When a rule expires (timeout) the next one is applied
- Rules are manually configured
- Recommendation: first rules should select more packets
  (taking benefit of the first instant before losing connectivity)

1: all outgoing IPv6 packets with a 10 second timeout
2: all outgoing IPv6 packets with a ratio of 10% and a 1 minute timeout
3: all outgoing multicast IPv6 packets with a ratio of 10% and a 1 minute timeout
...
Option encoding

- TLV-encoded in the IPv6 header

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Option type | Option Data Len | DOTS Signal Attribute[1] |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| DOTS Signal Attribute[2] | ... | DOTS Signal Attribute[n] |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- DOTS attributes
  - from draft-reddy-dots-transport
  - + a specific TTL value to avoid embedding the information into new packets indefinitely
  - + address and port of the DOTS server to reach (+ flags)
  - a mix between TLV and fixed-length fields

```
<table>
<thead>
<tr>
<th>Attribute type</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy-id</td>
<td>0</td>
</tr>
<tr>
<td>target-ip</td>
<td>1</td>
</tr>
<tr>
<td>target-port</td>
<td>2</td>
</tr>
<tr>
<td>target-protocol</td>
<td>3</td>
</tr>
<tr>
<td>lifetime</td>
<td>4</td>
</tr>
</tbody>
</table>
```
Deployment considerations 1/2

- IPv6 extension headers are often rate-limited or dropped entirely
  - One reason is the overhead of processing
  - Our proposed option is only used under a DDoS attack and performance might be so already degraded
  - Keep limited the use to the intra-domain use case

- Modification to IP layers implementations
  - capable routers: need to extract store and embed signaling information
  - clients: need to create the specific option header to be embedded then
  - servers and gateways: all DOTS signaling information contained in IPv6 headers has to transmitted to the application layer
Deployment considerations 2/2

- Need an interface for modifying/listening IPv6 packets
  - use of Hop-by-Hop option for applications → header violation
  - advanced socket API (RFC3542)
- Header insertion issue (rfc2460bis)
  - considered as harmful
  - potential solution by encapsulating into new packets
  - keep the use limited to routers under the same authority and make transparent packet modifications → fits well the intra-domain use case