Co-operative DDoS Mitigation

draft-reddy-dots-transport-05

July 2016

IETF 96

Authors: T. Reddy, D. Wing, P. Patil, M. Geller, M. Boucadair, R. Moskowitz

Presenter: Tirumaleswar Reddy
Changes to draft

• Meets most of the requirements in draft-ietf-dots-requirements-02
  ▪ Happy Eyeballs-like technique for DOTS Signal Channel (v6/v4, UDP/TCP)
  ▪ CoAP for lightweight communication
    ➢ DOTS Signal Channel, UDP/TCP
    ➢ DOTS Data Channel, TCP
  ▪ Mutual Authentication of DOTS Agents & Authorization of DOTS Clients
  ▪ (D)TLS protocol profile and Performance Considerations
Happy Eyeballs-like technique for DOTS Signal Channel

DOTS client

- DTLS ClientHello, IPv6
- TCP SYN, IPv6
- DTLS ClientHello, IPv4
- TCP SYN, IPv4
- DTLS ClientHello, IPv6
- TCP SYN, IPv6
- TCP SYN ACK, IPv4
- DOTS signal

DOTS server

- TLS Session
- DOTS signal
Happy Eyeballs for DOTS Signal Channel

• Order of preference (aligns with RFC6724)
  - IPv6 over DTLS over UDP
  - IPv6 over TLS over TCP
  - IPv4 over DTLS over UDP
  - IPv4 over TLS over TCP

• DNS lookup during peacetime.
DOTS signal and data channel

<table>
<thead>
<tr>
<th>DOTS</th>
<th>CoAP</th>
<th>TLS</th>
<th>DTLS</th>
<th>TCP</th>
<th>UDP</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DOTS signal channel

<table>
<thead>
<tr>
<th>DOTS</th>
<th>CoAP</th>
<th>TLS</th>
<th>TCP</th>
<th>IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

DOTS data channel
DOTS signal channel

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>Request to convey DOTS signal</td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
</tr>
<tr>
<td>PUT</td>
<td>Efficacy update from DOTS client</td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
</tr>
<tr>
<td>GET</td>
<td>Status of attack</td>
</tr>
<tr>
<td>200 OK</td>
<td>&quot;status&quot;: &quot;attack stopped&quot;</td>
</tr>
<tr>
<td>DELETE</td>
<td>Withdraw DOTS signal</td>
</tr>
<tr>
<td>200 OK</td>
<td></td>
</tr>
</tbody>
</table>
DOTS signal channel

- POST, DELETE, GET, and PUT requests are marked as COAP confirmable messages.
- Asynchronous message exchanges for DDOS mitigation status.
DOTS signal channel

DOTS client

GET <policy-id number>
Token: 0x4a
Observe: 0

2.05 content
Token: 0x4a
Observe: 12
Status: “mitigation in progress”

2.05 content
Token: 0x4a
Observe: 12
Status: “mitigation complete”

2.05 content
Token: 0x4a
Observe: 12
Status: “mitigation complete”

DOTS server
DOTS data channel

DOTS client

DOTS server

TLS Session

POST: filtering rules to black/white-list-list traffic

200 OK

Delete: remove filtering rules

200 OK
Mutual Authentication of DOTS agents

Example.com domain

Application Server (DOTS client)

Guest (DOTS client)

DDOS Detector (DOTS client)

(D)TLS for mutual authentication

Example.net domain

DOTS Gateway

DOTS Server

draft-reddy-dots-transport-05
Authorization of DOTS client

- Application Server (DOTS client)
- Guest (DOTS client)
- DDOS Detector (DOTS client)
- AAA Server
- DOTS Gateway
- DOTS Server

example.com domain

example.net domain
(D)TLS profile

• (D)TLS session resumption without server-side state [RFC5077].
• Raw public keys [RFC7250].
• (D)TLS Heartbeat.
Performance considerations

- TLS False Start [I-D.ietf-tls-falsestart].
- Cached Information Extension [I-D.ietf-tls-cached-info].
- TCP FastOpen [RFC7413].
Comments and questions
Consider adoption of this document as WG item.