DOTS Data Channel

https://github.com/boucadair/draft-ietf-dots-data-channel

DOTS WG Meeting
London, March 2018

Editors: Tiru (Reddy) & Med (Boucadair)
Agenda

• Pending Issues
• Next steps
List of Issues

• As per the agreement at the last Interim, a list of issues was shared on the mailing list to seek for feedback of a set of issues:
  – Issue #1: Lifetime handling
  – Issue #2: Filter Direction
  – Issue #3: Filter Activation
  – Issue #4: Filtering Fields
  – Issue #5: Scope of the filters
  – Issue #6: Multiple Servers
  – Issue #7: Loop Detect

• Update the github version to align with the latest versions of netmod-acl specification
Issue #1: Lifetime Handling

• It was agreed to associate a lifetime with entries instantiated by a DOTS client (-12):
  – A lifetime hint is included in the resource creation request by the client
  – The server may honor the suggested lifetime or assign a distinct value as per its local policies

• When a distinct value is used by the server, the issue is how to notify the client given that RFC8040 says:
  – "If the POST method succeeds, a "201 Created" status-line is returned and there is no response message-body."

• Conclusion
  – Servers must maintain an entry for a minimum period. Default is 1 week
  – No Lifetime is included in a request
  – Clients can retrieve the remaining lifetime using GET requests
  – If no refresh request is seen from the client, the server removes expired entries
Issue #2: Filter Direction

• Do we need to support explicit “direction” in filtering rules: “in”/“out”?

• Conclusion:
  – No
  – The current default direction is aligned with the nature of DDoS attacks targeted by DOTS (incoming)
    • ..even for the call home case
  – *No text change is required*
Issue #3: Filter Activation

• Do we assume that all filtering rules are activated by default or only when a mitigation is active?

• Conclusion:
  – We should support both
  – The intended action is governed by a new attribute called “activation-type” which can be set to “immediate” or “mitigation-time”
  – “mitigation-time” is the default value
Issue #4: Per-Domain or Per-client Filters?

• Do we consider filters created by a client are available to all clients of the domain, or just for the client?

• Conclusion
  – Filters that are activated only during mitigation time are on a per-client basis
    • Filters are per-domain when are immediately applied

• Open question
  – Should we mandate destination-network to be present for immediately enforced filters?
Issue #5: Filtering Fields

- Should we supporting all of the fields as defined by “ietf-packet-fields”?
  - Do we need to define a minimum supported set?

- Conclusion
  - List mandatory-to-support fields

<table>
<thead>
<tr>
<th>ACL Match</th>
<th>Mandatory Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>length, protocol, destination-ipv4-network, source-ipv4-network, and v4-fragments</td>
</tr>
<tr>
<td>ipv6</td>
<td>length, protocol, destination-ipv6-network, source-ipv6-network, and v6-fragments</td>
</tr>
<tr>
<td>tcp</td>
<td>flags, source-port-range-or-operator, and destination-port-range-or-operator</td>
</tr>
<tr>
<td>udp</td>
<td>length, source-port-range-or-operator, and destination-port-range-or-operator</td>
</tr>
<tr>
<td>icmp</td>
<td>type and code</td>
</tr>
</tbody>
</table>

- Define a capability containers to return the exact filtering capabilities of a server. Client MAY request the capabilities to adjust filtering requests sent to the server and avoid errors
Issue #6: Multiple Servers

• “If the request is propagated to both Servers, but one server sends back a different response code, what should be done?”

• Proposal
  – Current drafts focus on single-homed scenarios
    • Keep this focus
  – Multi-homing considerations are to be included in draft-boucadair-dots-multihoming
Issue #7: Loop Detect

• Same issue as for the signal channel

• Proposal
  – Re-use “max-forwards” header
    • ...but it is only for TRACE and OPTIONS
  – A loop-related http error that can be used is: 508(Loop Detected)

• Suggestions?
Working Copy

https://github.com/boucadair/draft-ietf-dots-data-channel
Next Steps

• Publish -14 with the changes agreed so far
• Any issues that are not covered?
• Questions?