Inter-Domain DOTS Use Cases

draft-nishizuka-dots-inter-domain-usecases-01

Kaname Nishizuka, NTT Communications
Apr. 2016 IETF95@Buenos Aires
Diff from -00 to -01

Revised Points:
1. Aligned with terminology of existing WG draft
2. Added studies about DDoS protection methods
3. Clarified the usecases
   • based on the feedback at the last IETF meeting and discussions given on the ML and direct messages
Categorization of use cases

1. intra-domain use cases
   • a DOTS client, a DOTS server and mitigators are in the same organization

2. inter-domain use cases
   • a DOTS server and mitigators are in a different organization from a DOTS client
     • 2-1. customer-to-provider(c2p)
     • 2-2. provider-to-provider(p2p)
Scenario of Inter-domain usecases

1. Provisioning of DDoS protection capability (if needed)
2. Attack Detection
3. DOTS Signaling
   - DOTS signaling from a DOTS client to a DOTS server in different organization
4. DDoS protection by mitigators
5. Protection Status
   - Status update from the DOTS server to the DOTS client
Protection methods

- For protection, these information should be provided from a DOTS client to a DOTS server

<table>
<thead>
<tr>
<th>Protection Method</th>
<th>Mandatory Information</th>
<th>Optional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blackholing</td>
<td>Destination Address</td>
<td></td>
</tr>
<tr>
<td>Selective Blackholing</td>
<td>Destination Address</td>
<td>BGP Community Next-hop Address</td>
</tr>
<tr>
<td>RTBH with uRPF</td>
<td>Source Address</td>
<td></td>
</tr>
<tr>
<td>BGP flowspec</td>
<td>Flow Type Action Rule</td>
<td></td>
</tr>
<tr>
<td>Filtering(ACL)</td>
<td>Match Rule Action Rule</td>
<td></td>
</tr>
<tr>
<td>DDoS mitigation Appliances</td>
<td>Destination Address</td>
<td>(Desired)Countermeasures Attack Telemetry</td>
</tr>
<tr>
<td>Detouring Technologies</td>
<td>Destination Address Next-Hop</td>
<td>Tunnel Information</td>
</tr>
</tbody>
</table>
Attack telemetry

- a set of summarized traffic information which characterizes the feature of the DDoS attack
- utilized by each protection methods

<table>
<thead>
<tr>
<th>Mandatory:</th>
<th>Dst IP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Optional:</th>
<th>Attack ID</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Dst Port</td>
</tr>
<tr>
<td></td>
<td>Src IP/Port</td>
</tr>
<tr>
<td></td>
<td>TCP Flag</td>
</tr>
<tr>
<td></td>
<td>Type of Attack</td>
</tr>
<tr>
<td></td>
<td>(Average/Maximum/Current)Traffic</td>
</tr>
<tr>
<td></td>
<td>Volume[bps/pps]</td>
</tr>
<tr>
<td></td>
<td>Severity</td>
</tr>
<tr>
<td></td>
<td>Attack Start Time</td>
</tr>
<tr>
<td></td>
<td>Duration</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DDoS Protection Status

- difficult to know whether the DDoS attack has ended or not from the monitoring point of the DOTS client especially if it is inter-domain
- Information from DOTS server to client
  - Attack telemetry
  - Status of protection
  - Data for billing
Inter-domain usecases

• Customer to Provider (c2p)
  • Usecase 1: Single-home Model
  • Usecase 2: Multi-home Model

• Provider to Provider (p2p)
  • Usecase 3: Delegation Model
  • Usecase 4: Distributed Architecture Model
  • Usecase 5: Centralized Architecture Model

Multi-provider cooperative DDoS protection
→ draft-nishizuka-dots-inter-domain-mechanism
Inter-domain usecase 1: Single-home model

Diagram:
- Domain A
  - DOTS Client
  - DOTS signaling (Attack telemetry)
- Domain B
  - DOTS Server
  - Mitigators
  - Attackers
  - Legitimate traffic
- Customer
- Provider
- Victim
Inter-domain usecase2: Multi-home model
Inter-domain usecase3: Delegation model
Inter-domain usecase4: Distributed Architecture model
Inter-domain usecase5: Centralized Architecture model
Nextstep

• Consolidation with draft-ietf-dots-use-cases-01
  • Texts and contexts will be merged