Efficient use of DMS based on traffic bandwidth: DOTS Telemetry use case

IETF#106, Singapore, November 2019

Yuhei Hayashi (NTT)
Summary of Presentation

• We carried out a PoC about efficient use of DMS based on traffic bandwidth.
• We assessed that DOTS telemetry spec, especially YANG module related toptalker & bandwidth, can be applied in the use case.
Assumption

Role of Flow Collector
- Detecting DDoS attack, target \((dst_ip)\) and attackers (list of \(src_ip\)).
- Reporting the \((dst_ip, src_ip)\) tuple flows of attack with bandwidth.

![Diagram showing network components and their roles in detecting and mitigating DDoS attacks.](image)
**Use case Scenario**

*PoC of this scenario was already done in our labs.*

**Role of Orchestrator**
- Receiving attack report and checking the duplication.
- Registering bandwidth of \((dst_ip, src_ip)\) tuple flows.
- Checking available capacity of DMS.
- Checking if the \(dst_ip\) is DMS service subscriber’s one.
- Redirecting attack flow to DMS.
  
  IF DMS available capacity > \((dst_ip)\) flow’s bandwidth.
  
  Redirecting \((dst_ip)\) flow to available DMS.
  
  ELSE
  
  Redirecting \((dst_ip, src_ip)\) tuple flows of top-talker.

**Role of Selector**
- Accommodating the flow to the available DMS.

**Diagram**
- Provider Network
- Attacker
- PE Router
- Core Router
- Flow Collector
- Orchestrator
- Scrubbing Center
- DMS
- Target (DMS Service Subscriber)

NetFlow
- Attack Report
- Redirect Signal (bgp/bgpflowspec etc.)
Assessment of DOTS Telemetry

Theoretically, the YANG module related top-talker & bandwidth can be applied to the use case.

**Role of Orchestrator**
- Receiving attack report and checking the duplication.
- Registering bandwidth of \((dst_ip, src_ip)\) tuple flows.
- Checking available capacity of DMS.
- Checking if the \(dst_ip\) is DMS service subscriber’s one.
- Redirecting attack flow to DMS.
  - IF DMS available capacity > \((dst_ip)\) flow’s bandwidth.
  - Redirecting \((dst_ip)\) flow to available DMS.
- Redirecting \((dst_ip, src_ip)\) tuple flows of top-talker.

**Excerpt a quote from draft-reddy-dots-telemetry-04**

```
augment /ietf-signal:dots-signal/ietf-signal:message-type: +--:(telemetry) {dots-telemetry}]?
  ...
  +--rw pre-mitigation* [telemetry-id]
  +--rw telemetry-id
  +--rw target
  |  +--rw target-prefix*
  ...
  |  +--ro total-attack-traffic*
  +--ro attack-detail
  ...
  +--ro top-talker
  +--ro source-prefix*
  ...
  +--ro source-prefix
  +--ro total-attack-traffic*
  ...
```