DOTS Telemetry Use Cases

draft-hayashi-dots-telemetry-use-cases-00

interim-2020-dots-01

Yuhei Hayashi
Meiling Chen

Back Ground

- At IETF106, we presented a telemetry use case*1 and some people suggested us to write telemetry use case draft.

- We merged telemetry use cases proposed by CMCC*2.

*1 https://datatracker.ietf.org/meeting/106/materials/slides-106-dots-dots-telemetry-usecase-00.pdf
*2 https://datatracker.ietf.org/meeting/104/materials/slides-104-dots-attack-bandwidth-and-attack-type-expansion-01.pdf

Objective & Contents

Objective of the draft

- Showing how to use DOTS Telemetry in a network.
- Diffusion of DOT telemetry.

Contents of the draft

- Sample use cases for DOTS Telemetry in the network.
    - Aim of the use case.
    - What components are deployed in the network.
    - How they cooperate.
    - What information is exchanged.

Sample Use Cases

Signal directions of all use cases are C -> S.

Use Case Name		DOTS Client	DOTS Server	Essential Attribute	Mitigator
Based on Attack Traffic Bandwidth	Mitigating Attack Flow of Top-talker Preferentially *1	Flow Collector	Orchestrator	- target-prefix - top-talkers	Forwarding Node DMS
	Optimal DMS Selection for Mitigation *2	Flow Collector	Orchestrator	- target-prefix - total-attack-traffic	Forwarding Node DMS
	Best-path Selection for Redirection *2	Flow Collector	Orchestrator	- target-prefix - total-attack-traffic	Forwarding Node DMS
		Forwarding Node	Orchestrator	- total-traffic - total-pipe-capability	Forwarding Node DMS
	Short but Extreme Volumetric Attack Mitigation *2	Network Management System	Administrative System	- target-prefix - total-pipe-capability - total-attack-traffic	Forwarding Node
Based on Attack Type	Selecting Mitigation Technique *3	Flow Collector	Orchestrator	- target-prefix - attack-name *4	Forwarding Node DMS
The other	Training Flow Collector Using Supervised Machine Learning *3	DMS	Flow Collector	- target-prefix - top-talkers	DMS

*1 https://datatracker.ietf.org/meeting/106/materials/slides-106-dots-dots-telemetry-usecase-00.pdf
*2 https://datatracker.ietf.org/meeting/104/materials/slides-104-dots-attack-bandwidth-and-attack-type-expansion-01.pdf
*3 New use cases *4 {vendor-id, attack-id} can also be used.

Status of Use of Telemetry Attributes

```
augment /ietf-signal:dots-signal/ietf-signal:message-type:
  +--:(telemetry-setup) {dots-telemetry}?
  |    ...
  |      +--rw (setup-type)?
  |         +--:(telemetry-config)
  |         |  ...
  |         +--:(pipe)
  |         | ...
  |         +--:(baseline)
  |         ...
  +--:(telemetry) {dots-telemetry}?
     +--rw pre-or-ongoing-mitigation* [cuid tmid]
           ...
        +--rw target
        |  ...
        +--rw total-traffic* [unit]
        |  ...
        +--rw total-traffic-protocol* [unit protocol]
        |  ...
        +--rw total-traffic-port* [unit port]
        |  ...
        +--rw total-attack-traffic* [unit]
        |  ...
        +--rw total-attack-traffic-protocol* [unit protocol]
        |  ...
        +--rw total-attack-traffic-port* [unit port]
        |  ...
        +--rw total-attack-connection
        |  ...
        +--rw total-attack-connection-port
        |  ...
```

```
+--rw attack-detail* [vendor-id attack-id]
   +--rw vendor-id            uint32
   +--rw attack-id            uint32
   +--rw attack-name?         string
   +--rw attack-severity?     attack-severity
   +--rw start-time?          uint64
   +--rw end-time?            uint64
   +--rw source-count
   +--rw top-talker
   ...
```

draft-ietf-dots-telemetry-09

: at least one use case uses

ToDo

- Adding additional use cases
  - Usage of baseline and total-attack-connections and so on.
  - Signaling from server to client

- Addressing comments from WG
  - Comments and co-authors are welcome!

Discussion

Some options on how to move forward with this draft.

Opt 1. Require WG adoption after addressing comments from WG.
-> Some people prefer on ML.

Opt 2. Add a high-level use case description to the Telemetry draft.
(e.g. Appendix)
-> Chair said this is better.
https://datatracker.ietf.org/doc/minutes-106-dots/