DOTS Telemetry

https://datatracker.ietf.org/doc/draft-ietf-dots-telemetry/

June 2020

Agenda

• Status
• Zoom on some key design points
• Next Steps
Changes

• 12/19: WG Adoption
• 9 Revisions since then
  – 42 (00) vs. 105 pages (09)
  – 1 (00) vs. 2 YANG modules (09)
  – 51 (00) vs. 117 attributes (09)
  – +40 Examples/Figures in 09
  – Integrated implementation feedback
• We won’t list all the changes but we will focus on some of them
When to Share Telemetry Data: Some Samples

DOTS Client

Mitigation Request (mid)

DOTS Server

Share attack information to foster mitigation

Telemetry (target=mid)
When to Share Telemetry Data: Some Samples

DOTS Client

An attack is detected on a resource bound to the DOTS client

Telemetry (target-prefix)

Check if the attack can be handled locally

Mitigation Request (target-prefix)

DOTS Server
How to Share Telemetry Data

augment /ietf-signal:dots-signal/ietf-signal:message-type:
...
+++:(telemetry) {dots-telemetry}?
   +++-rw pre-or-ongoing-mitigation* [cuid tmid]
      +++-rw cuid       string
      +++-rw cdid?      string
      +++-rw tmid       uint32
      +++-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]
     ...

NEW Operation Path= /tm

Used to bind telemetry data with a mitigation request

Comprehensive set of data. The granularity is controlled by DOTS agents
When to Share Telemetry Data:
Some Samples (Con’d)

DOTS Client

Mitigation Request (mid)

DOTS Server

Share attack information
for better attack
coordination

Efficacy Update (+Telemetry Data)

augment /ietf-signal:dots-signal/ietf-signal:message-type
   /ietf-signal:mitigation-scope/ietf-signal:scope:
   +++rw total-attack-traffic* [unit] {dots-telemetry}?
   | ...
   +++rw attack-detail* [vendor-id attack-id] {dots-telemetry}?
       +++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
   ...

...
When to Share Telemetry Data:
Some Samples (Con’d)

DOTS Client

Mitigation Request (mid)

DOTS Server

Status Update (+ Telemetry Data)

Share attack details

Only aggregates are included

```
augment /ietf-signal:dots-signal/ietf-signal:message-type
 /ietf-signal:mitigation-scope/ietf-signal:scope:
  +---ro total-traffic* [unit] {dots-telemetry}?  
  |   ...                                        
  +---rw total-attack-traffic* [unit] {dots-telemetry}?  
  |   ...                                        
  +---ro total-attack-connection {dots-telemetry}?  
  |     ...                                       
  |       +---ro low-percentile-c 
  |       |   ... 
  |       +---ro mid-percentile-c 
  |       |   ... 
  |       +---ro high-percentile-c 
  |       |   ... 
  |       +---ro peak-c 
  |       ...                                      
  +---rw attack-detail* [vendor-id attack-id] {dots-telemetry}?  
```

Only aggregates are included
When to Share Telemetry Data: Some Samples (Con’d)

DOTS Client

DOTS Server

Telemetry (Share Normal Traffic Baseline)

Can be used to detect abnormal traffic

Comprehensive set of data

```
augment /ietf-signal:dots-signal/ietf-signal:message-type:
  +--:(telemetry-setup) {dots-telemetry}?
    |    ...
    |   +--:(baseline)
    |    |   +--rw baseline* [id]
    |    |     +--rw id uint32
    |    |     +--rw target-prefix* inet:ip-prefix
    |    |     +--rw target-port-range* [lower-port]
    |    |     |...+
    |    |     +--rw target-protocol* uint8
    |    |     +--rw target-fqdn* inet:domain-name
    |    |     +--rw target-uri* inet:uri
    |    |     +--rw alias-name* string
    |    |     +--rw total-traffic-normal* [unit]
    |    |     |...+
    |    |     +--rw total-traffic-normal-per-protocol* [unit protocol]
    |    |     |...+
    |    |     +--rw total-traffic-normal-per-port* [unit port]
    |    |     |...+
    |    |     +--rw total-connection-capacity* [protocol]
    |    |     |...+
    |    |     +--rw total-connection-capacity-per-port* [protocol port]
    |    |     ...
```
When to Share Telemetry Data: Some Samples (Con’d)

DOTS Client

DOTS Server

Telemetry (Pipeline)

| augment /ietf-signal:dots-signal/ietf-signal:message-type: |
| +--:(telemetry-setup) {dots-telemetry}? |
| | ... |
| | +--:(pipe) |
| | | +--rw total-pipe-capacity* [link-id unit] |
| | | +--rw link-id nt:link-id |
| | | +--rw capacity uint64 |
| | | +--rw unit unit |
| | ... |

Avoid overloading incoming links when forwarding « clean » traffic

Applies for the DOTS client domain
Telemetry Configuration

```
augment /ietf-signal:dots-signal/ietf-signal:message-type:
  +--:(telemetry-setup) {dots-telemetry}?
    |   +--ro max-config-values
    |   |   +--ro measurement-interval? interval
    |   |   +--ro measurement-sample? sample
    |   |   +--ro low-percentile? percentile
    |   |   +--ro mid-percentile? percentile
    |   |   +--ro high-percentile? percentile
    |   |   +--ro server-originated-telemetry? boolean
    |   |   +--ro telemetry-notify-interval? uint32
    |   +--ro min-config-values
    |      +...
    |   +--ro supported-units
    |   |   +--ro unit-config* [unit]
    |   |   |   +--ro unit unit-type
    |   |   |   +--ro unit-status boolean
    |   |   +--ro query-type* query-type
    |   |      +--rw (setup-type)?
    |   |      |   +--:(telemetry-config)
    |   |      |      |   +...
    |   |      |   +--:(pipe)
    |   |      |      |   +...
    |   |      |   +--:(baseline)
    |   |      |      |...+
    |   +--:(telemetry) {dots-telemetry}? ...
```

Controls whether the server can include telemetry data in the status update

Controls the pace of telemetry notifications
One or Two Key Values?

```
"ietf-dots-telemetry:total-attack-traffic": [ 
  { 
    "ietf-dots-telemetry:unit": "megabit-ps",
    "ietf-dots-telemetry:mid-percentile-g": "900"
  }
]
```

```
"total-attack-traffic": [ 
  { 
    "unit": "megabit-ps",
    "mid-percentile-g": "900"
  }
]
```
### One or Two Key Values?

```
"ietf-dots-telemetry:total-attack-traffic": [ 
  { 
    "ietf-dots-telemetry:unit": "megabit-ps",
    "ietf-dots-telemetry:mid-percentile-g": "900"
  }
]
```

```
"total-attack-traffic": [ 
  { 
    "unit": "megabit-ps",
    "mid-percentile-g": "900"
  }
]
```

| Parameter Name       | YANG        | CBOR | CBOR Major Type & Information | JSON   |
|----------------------+-------------+------+--------------------------------+--------|
| total-attack-traffic | list        | TBA17 | 4 array                        | Array  |
| ietf-dots-telemetry: |             |      |                                |        |
| total-attack-traffic | list        | TBA87 | 4 array                        | Array  |
Telemetry Attributes

• Comprehension-Required or Comprehension-Optional?
Telemetry Attributes

• Comprehension-Required or Comprehension-Optional?
  – Telemetry data are hints
  – Should not exacerbate message processing failures
  – Consistent with other specs (e.g., "source-prefix")

• This has an implication on the size as the key values will consume 3 bytes; hence this proposal:

<table>
<thead>
<tr>
<th>Range</th>
<th>Registration Procedures</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-127</td>
<td>IETF Review</td>
<td>comprehension-required</td>
</tr>
<tr>
<td>128-255</td>
<td>IETF Review</td>
<td>comprehension-optional</td>
</tr>
<tr>
<td>255-16383</td>
<td>IETF Review</td>
<td>comprehension-required</td>
</tr>
</tbody>
</table>

Any objection?
Minimize the Size of Telemetry Data

- Filter out the asynchronous notifications (Uri-Query)
- Share the attack mapping details

```
module: ietf-dots-mapping
  augment /ietf-data:dots-data/ietf-data:dots-client:
    +++rw vendor-mapping {dots-telemetry}?
    +++rw vendor* [vendor-id]
    +++rw vendor-id uint32
    +++rw attack-mapping* [attack-id]
    +++rw attack-id uint32
    +++rw attack-name string

augment /ietf-data:dots-data/ietf-data:capabilities:
  +++ro vendor-mapping-enabled? boolean {dots-telemetry}?

augment /ietf-data:dots-data:
  +++ro vendor-mapping {dots-telemetry}?
  +++ro vendor* [vendor-id]
  +++ro vendor-id uint32
  +++ro attack-mapping* [attack-id]
  +++ro attack-id uint32
  +++ro attack-name string
```

Avoids the need to include this attribute in the signal channel message
Oversized Packet Handling

• Application break up data into Chunks
  – YANG <anydata> requires chunk to be full JSON as per RFC7951
  – How to break data down to minimize number of chunks?

• Use BLOCK1 and BLOCK2: Has limitations
  – Performance (symmetric traffic requires ‘ACK’ before next block is sent)
  – Handling lossy environments

• Use BLOCK3 and BLOCK4: Faster transmission without Block1/Block2 issues
Block3/Block4 Options
draft-bosh-core-new-block

- Applicability Scope: DOTS-like
- Guards to prevent a CoAP agent from overloading the network
  - PROBING_RATE clarification
  - MAX_PAYLOADS defined, with a default value of 10

- Detailed description of Block3/Block4 Option
  - Including the use of Etag and Request-Tag
- New CoAP Response Code for missing blocks
Block3: An Example

CoAP Client | CoAP Server
| | |
+-------->| NON PUT /path M:0x05 T:0xe0 RT=11 B3:0/1/1024
+--->X | NON PUT /path M:0x06 T:0xe1 RT=11 B3:0/1/1/1024
+--->X | NON PUT /path M:0x07 T:0xe2 RT=11 B3:0/2/1/1024
+-------->| NON PUT /path M:0x08 T:0xe3 RT=11 B3:0/3/0/1024

[[Server realizes missing blocks and indicates this]]
|<--------+ NON 4.18 M:0xf2 T:0xe3 [Missing 1,2 for RT=11]
+-------->| NON PUT /path M:0x09 T:0xe4 RT=11 B3:0/1/1/1024
+--->X | NON PUT /path M:0x0a T:0xe5 RT=11 B3:0/2/1/1024

[[Server requests final missing block]]
|<--------+ NON 4.18 M:0xf3 T:0xe4 [Missing 2 for RT=11]
+-------->| NON PUT /path M:0x0b T:0xe6 RT=11 B3:0/2/1/1024
|<--------+ NON 2.04 M:0xf4 T:0xe6
CoAP      CoAP
Client    Server
|         |
...

[[Observe triggered]]
|<----------+ NON 2.05 M:0xf9 T:0xf0 O:1236 ET=23 B4:0/1/1024
|    X<----+ NON 2.05 M:0xfa T:0xf0 O:1236 ET=23 B4:1/1/1024
|    X<----+ NON 2.05 M:0xfb T:0xf0 O:1236 ET=23 B4:2/1/1024
|<----------+ NON 2.05 M:0xfc T:0xf0 O:1236 ET=23 B4:3/0/1024

[[Client realizes blocks are missing and asks for the missing ones in one go]]
+---------->| NON GET /path M:0x02 T:0xf1 ET=23 B4:/1/0/1024 \ 
|    |      B4:2/0/1024
|    X<----+ NON 2.05 M:0xfd T:0xf1 ET=23 B4:1/1/1024
|<----------+ NON 2.05 M:0xfe T:0xf1 ET=23 B4:2/1/1024

[[Client gets final missing block]]
+---------->| NON GET /path M:0x03 T:0xff ET=23 B4:1/0/1024 
|<----------+ NON 2.05 M:0xff T:0xff ET=23 B4:1/1/1024
Current Discussion in the Draft

DOTS clients can use Block-wise transfer [RFC7959] with the recommendation detailed in Section 4.4.2 of [RFC8782] to control the size of a response when the data to be returned does not fit within a single datagram.

DOTS clients can also use CoAP Block1 Option in a PUT request (see Section 2.5 of [RFC7959]) to initiate large transfers, but these Block1 transfers will fail if the inbound "pipe" is running full, so consideration needs to be made to try to fit this PUT into a single transfer, or to separate out the PUT into several discrete PUTs where each of them fits into a single packet.

Block3 and Block 4 Options that are similar to the CoAP Block1 and Block2 Options, but enable faster transmissions of big blocks of data with less packet interchanges, are defined in [I-D.bosh-core-new-block]. DOTS implementations can consider the use of Block3 and Block 4 Options.

No normative language is used on purpose
Implementation & Interop
Implementation Status (Jon)

- RFC8782: DOTS Signal Channel Specification
- RFC8783: DOTS Data Channel Specification
- RFC8768: CoAP Hop-Limit Option
- draft-ietf-dots-signal-filter-control-06
- draft-ietf-dots-signal-call-home-08
- draft-ietf-dots-server-discovery-10
- draft-ietf-dots-telemetry-07
  - Currently using Block2 if needed (8.1 may trigger Block1 usage)
  - Still in the process of implementing the vendor-id/attack-id changes to bring things up to the -09 spec
godots (Kaname)

• RFCs
  – RFC 8782 / RFC 8783
• drafts
  – draft-ietf-dots-signal-filter-control-06
  – draft-ietf-dots-signal-call-home-08
  – draft-ietf-dots-telemetry-09 <- Today’s topic
Interop (Kaname/Jon)

• Interoperability test of dots-telemetry has been done intensively on March/April
• Issues were fixed at both ends
• Essentially Sections 6, 7, and 8 were ‘working’
  – Sections 6.5 and 8.1 still to be done
• General conclusion was that this was useful to have to pass back and forth additional information
# DOTS Telemetry Coverage

<table>
<thead>
<tr>
<th>Section</th>
<th>godots</th>
<th>Interop tests</th>
<th>NCC</th>
</tr>
</thead>
<tbody>
<tr>
<td>6. DOTS Telemetry Setup Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1 Telemetry Configuration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2 Total Pipe Capacity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3 Telemetry Baseline</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4 Reset Installed Telemetry Setup</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.5 Conflict with Other DOTS Clients of the Same Domain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. DOTS Pre-or-Ongoing Mitigation Telemetry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.1 Pre-or-Ongoing-Mitigation DOTS Telemetry Attributes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.2 From DOTS Clients to DOTS Servers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.3 From DOTS Servers to DOTS Clients</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. DOTS Telemetry Mitigation Status Update</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.1 DOTS Clients to Servers Mitigation Efficacy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.2 DOTS Servers to Clients Mitigation Status</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Not tested:
- Block-wise transfer Block3/Block4 (4.5)
- Vendor attack mapping(7.1.5)
In summary

No significant issue is found but some functionality needs clarification

1. Current Uri-Path can't distinguish telemetry resources posted by the client or created by the server.
   - Those are totally different resources. For example, Uri-Query won't be applicable to the telemetry resources posted by the client.

Proposal: Kaname to identify precisely which parts of the text need to be updated. Will then discuss whether/which changes are required.
In summary

No significant issue is found but some functionality needs clarification

1. Current Uri-Path can't distinguish telemetry resources posted by the client or created by the server.

2. Is the created vendor mapping shared among different DOTS clients?

   | module: ietf-dots-data-channel |
   | ---rw dots-data |
   | ---rw dots-client* [cuid] |
   |     +---rw cuid  | string |

   | module: ietf-dots-mapping |
   | augment /ietf-data:dots-data/ietf-data:dots-client: |
   | ---rw vendor-mapping {dots-telemetry} |

DOTS clients of the same domain may interface with distinct DDoS protection technologies. Will add some text to better reflect this.
In summary

No significant issue is found but some functionality needs clarification

1. Current Uri-Path can't distinguish telemetry resources posted by the client or created by the server.
2. Is the created vendor mapping shared among different DOTS client?
3. "DOTS agents MUST NOT include 'attack-name' attribute except if the corresponding attack mapping details were not shared with the peer DOTS agent". But how can the DOTS server know they're shared or not?

- Clarification: This is implementation-specific. The DOTS server may record which version of the mapping table it shared with a DOTS client.
- Question: Do you think that we need to touch on these details?
Next Steps

• Release -10 with any required fixes to take into account in particular the implementation feedback and any comments raised today

• WGLC on -10