Revision Letter for Consumer-Facing Interface YANG Data Model

March 26, 2023
Editor: Jaehoon Paul Jeong

OLD: draft-ietf-i2nsf-consumer-facing-interface-dm-26
NEW: draft-ietf-i2nsf-consumer-facing-interface-dm-27

Dear Tom Petch and Joseph Touch,

I sincerely appreciate your comment to improve our Consumer-Facing Interface YANG Data Model. I use bold font for your comment and use a regular blue font for my responses with the prefix “=> [PAUL]”.

[Comments from Tom Petch]

Belatedly I notice another area of divergence which makes the set of documents incoherent and that is with threats.

This I-D uses 'ioc' as a basis' from which is derived

```
      identity stix {
      identity misp {
      identity openioc {
      identity iodef {
```

Earlier versions used threat feed with

```
      identity signature-yara {
      identity signature-snort {
      identity signature-suricata {
```

and the capability I-D, with the RFC Editor, has

```
      identity content-security-control {
```

which derives

```
     identity ips {
     identity anti-virus {
```

which give rise to

```
      identity signature-set {
      identity exception-signature {
```

and

```
      identity detect {
```

```
      identity exception-files {
```

I am unclear how the capabilities which can be configured in this I-D are specified with the YANG identity of the capability I-D. A sentence or two in this I-D explaining the relationship might clarify.

=> [PAUL] We added a paragraph explaining the relationship between this I-D and the capability I-D in terms of Indicators of Compromise (IOC) for threat feed as follows:

NEW:

5.1. Threat Feed

This object represents a threat feed which provides the signatures of malicious activities. Figure 16 shows the YANG tree of a Threat-feed-list. The Threat-Feed object SHALL have the following information:

Name: This field identifies the name of this object.

IOC: This field represents the Indicators of Compromise (IOC), i.e., the critical information of patterns or characteristics in the threat feed that identifies malicious activities. The format of the information given in this field is based on the format field (e.g., STIX, MISP, OpenIOC, and IODEF).

Format: This field represents the format or structure of the IOC field for the threat-feed such as Structured Threat Information Expression (STIX) [STIX], MISP Core [MISPCORE], OpenIOC [OPENIOC], and Incident Object Description Exchange Format (IODEF) [RFC8727]. This can be extended depending on the implementation of the existing threat-feed.

It is assumed that the I2NSF User obtains the threat signatures (i.e., threat content patterns) from a threat-feed server (i.e., feed provider), which is a server providing threat signatures. With the obtained threat signatures, the I2NSF User can deliver them to the Security Controller via the Consumer-Facing Interface. The retrieval of the threat signatures by the I2NSF User is out of the scope of this document.

Note that the information of a threat feed (i.e., a pair of IOC and Format) is used as information to alert or block traffic that matches IOCs identified in the threat feed. This information is used to update the NSFs that have various content security control capabilities (e.g., IPS, URL-Filtering, Antivirus, and VoIP/VoCN Filter) derived in [I-D.ietf-i2nsf-capability-data-model]. Those capabilities derive specific content security controls such as signature-set, exception-signature, and detect.

```
     +--rw threat-feed-list* [name]
     |  +--rw name      string
     |  +--rw ioc*      string
     |  +--rw format    identityref
```

Figure 16: Threat Feed YANG Data Tree

Tom Petch

[Comments from Joseph Touch]

Reviewer: Joseph Touch
Review result: Ready with Issues

This document has been reviewed as part of the transport area review team's ongoing effort to review key IETF documents. These comments were written primarily for the transport area directors, but are copied to the document's authors and WG to allow them to address any issues raised and also to the IETF discussion list for information.

When done at the time of IETF Last Call, the authors should consider this review as part of the last-call comments they receive. Please always CC tsv-art@ietf.org if you reply to or forward this review.

Note that this review focuses on transport issues. The document's content has not been otherwise reviewed.

Overall, there is little transport-related content in this document. As a YANG model, there are no transport issues.

The model itself does refer to transport protocols by name. The list is sufficiently complete.

The only key issue is the reference to ways of blocking protocols. The "identity reject" entry below describes a variety of ways of blocking transport protocols, but these examples have issues. It is important that this document be updated to give correct advice, even if in such examples.

> ...For example, a TCP packet is rejected with
> TCP RST response or a UDP packet may be rejected with an
> ICMPv4 response message with Type 3 Code 3 or ICMPv6 response
> message Type 1 Code 4 (i.e., Destination Unreachable:
> Destination port unreachable)."

It is not entirely clear from the rest of the context of this document, but if this filtering occurs anywhere other than the destination IP address of these packets then ICMP messages from routers should be used, not those from hosts. I.e., if the issue is packets to/from a NFV service, then host errors are appropriate, but if the issue is packets relayed through an NFV service, then router errors should be used instead.

Additionally, assuming host errors are intended, the entry mentions ICMPv4 Type

3 Code 3 (Destination port unreachable) and ICMPv6 Type 1 Code 4 (also Destination port unreachable), where it appears that ICMPv4 Type 3 Code 10 and ICMPv6 Type 1 Code 1 (both “administratively prohibited”) seems more appropriate.

That entry also incorrectly refers to use of TCP RST. TCP RST should be reserved for actions of the receiver TCP protocol engine based on state errors, and emitting that message requires that endpoint’s TCP to enter TIME-WAIT for that socket pair (RFC 9293, Note 3 in Sec 3.3). It should never be issued by a third party that might not be in a position to maintain those TIME-WAIT states. It is also not clear it is appropriate to reject connections using this technique, i.e., as a substitute for host ICMPs.

=> [PAUL] To address the above comments, we have updated the description of “identity reject” where a packet should be rejected with ICMPv4 Type 3 Code 13 or ICMPv6 Type 1 Code 1 as follows:

NEW:

```
  identity reject {
    base ingress-action;
    base egress-action;
    description
      "The reject action denies a packet to go through the NSF
       entering or exiting the internal network and sends a response
       back to the source. The response depends on the packet and
       implementation. For example, a packet may be rejected with
       an ICMPv4 Type 3 Code 13 or ICMPv6 Type 1 Code 1 reply message
       (i.e., Destination Unreachable: Communication Administratively
       Prohibited) by an administrative purpose (e.g., firewall
       filter).";
  }
```

I sincerely appreciate the valuable comments to improve the document.

Best Regards,
Jaehoon (Paul) Jeong