Revision Letter

I2NSF Capability YANG Data Model

(Old Draft Name: draft-ietf-i2nsf-capability-data-model-04 and New Draft Name: draft-ietf-i2nsf-capability-data-model-05)

Jaehoon Paul Jeong

07/25/2019

Hi Acee,

I sincerely appreciate your detailed review on this draft. Your comments use a bold font and my answers use a regular font, starting with the mark “=> [Paul]”.

Document: draft-ietf-i2nsf-capability-data-model-04.txt

Reviewer: Acee Lindem

Review Date: June 18, 2019

Review Type: Working Group Last Call

Intended Status: Standards Track

Summary: Not ready for publication

Modules: "ietf-i2nsf-capability@2019-03-28.yang"

Tech Summary: The model is logically structured and seems to fulfill its intended purpose. The "Overview" section defines the usage, context, and usage of the model, i.e., it is limited to the NSF capability registration interface. However, the draft/model is very rough and not ready for working group last call. It seems that it has not gotten adequate review by the chairs and other members of the I2NSF Working Group.

Major Comments:

1. The "Security Considerations" in section 8 do not conform to the recommended template in https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines>

=> [PAUL] I revised “Security Considerations” Section according to the recommended template.

OLD:

The YANG module specified in this document defines a data schema designed to be accessed through network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040].

The lowest NETCONF layer is the secure transport layer, and the required transport secure transport is Secure Shell (SSH) [RFC6242].

The lowest RESTCONF layer is HTTPS, and the required transport secure transport is TLS [RFC8446].

The NETCONF access control model [RFC8341] provides a means of restricting access to specific NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

NEW:

The YANG module specified in this document defines a data schema designed to be accessed through network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040].

The lowest NETCONF layer is the secure transport layer, and the required transport secure transport is Secure Shell (SSH) [RFC6242].

The lowest RESTCONF layer is HTTPS, and the required transport secure transport is TLS [RFC8446].

The NETCONF access control model [RFC8341] provides a means of restricting access to specific NETCONF or RESTCONF users to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

There are a number of data nodes defined in this YANG module that are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., edit-config) to these data nodes without proper protection can have a negative effect on network operations. These are the subtrees and data nodes and their sensitivity/vulnerability:

- ietf-i2nsf-capability: The attacker may provide incorrect information of the security capability of any target NSF by illegally modifying this.

Some of the readable data nodes in this YANG module may be considered sensitive or vulnerable in some network environments. It is thus important to control read access (e.g., via get, get-config, or notification) to these data nodes. These are the subtrees and data nodes and their sensitivity/vulnerability:

- ietf-i2nsf-capability: The attacker may gather the security capability information of any target NSF and misuse the information for subsequent attacks.

2. The document is missing XML or JSON examples.

=> [PAUL] I added the XML examples according to your comments in the Section Appendix A. Configuration Examples.

Minor Comments:

1. Section 3.1 should reference RFC8340 rather than attempting to include tree diagram formatting semantics.

=> [PAUL] I deleted tree diagram formatting semantics, and let the section have a reference to RFC8340.

OLD:

3.1. Tree Diagrams

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in these diagrams [RFC8340] is as follows:

- Brackets "[" and "]" enclose list keys.
- Abbreviations before data node names: "rw" means configuration (read-write) and "ro" state data (read-only).
- Symbols after data node names: "?" means an optional node and "*" denotes a "list" and "leaf-list".
- Parentheses enclose choice and case nodes, and case nodes are also marked with a colon (":").
- Ellipsis ("...") stands for contents of subtrees that are not shown.

NEW:

3.1. Tree Diagrams
A simplified graphical representation of the data model is used in this document. The meaning of the symbols in these diagrams is referred from [RFC8340]

2. Much of the text is very hard to read and awkwardly worded. There are some instances of sentence fragments. I starting trying to remedy this but found I was rewriting the entire draft and, in many cases, I wasn't sure my edits matched the original intent. See the attached diff with suggested edits.

=> [PAUL] I reflected your suggested text to improve the wording.

3. "iicapa" is a poor choice for default model prefix - I suggest "nsfcap". It is just as concise but actually expands to something meaningful.

=> [PAUL] I agree at your comments on replacing “iicapa” with “nsfcap”.

OLD:

7. IANA Considerations

This document requests IANA to register the following URI in the "IETF XML Registry" [RFC3688]:

URI: urn:ietf:params:xml:ns:yang:ietf-i2nsf-capability

Registrant Contact: The IESG.

XML: N/A; the requested URI is an XML namespace.

This document requests IANA to register the following YANG module in the "YANG Module Names" registry [RFC7950].

name: ietf-i2nsf-capability

namespace: urn:ietf:params:xml:ns:yang:ietf-i2nsf-capability

prefix: iicapa

reference: RFC XXXX

NEW:

7. IANA Considerations

This document requests IANA to register the following URI in the "IETF XML Registry" [RFC3688]:

URI: urn:ietf:params:xml:ns:yang:ietf-i2nsf-capability

Registrant Contact: The IESG.

XML: N/A; the requested URI is an XML namespace.

This document requests IANA to register the following YANG module in the "YANG Module Names" registry [RFC7950].

name: ietf-i2nsf-capability

namespace: urn:ietf:params:xml:ns:yang:ietf-i2nsf-capability

prefix: nscap

reference: RFC XXXX

4. Similar to the text in the narrative sections of the draft, the text in the YANG model description statements is very awkwardly worded.

=> [PAUL] I revised the wording according to your comments.

5. What are the references for the ipv4-sameip and ipv4-geoip conditions?

=> [PAUL] I deleted the ipv4-sameip because it is not needed, and added a reference to the ipv4-geoip-conditions.

NEW:

```
identity ipv4-geoip {
    base ipv4-capa;
```

```
    description
      "Identity for geography capability
      of IPv4 condition";
    reference
      "draft-ietf-i2nsf-capability-04: Information Model
       of NSFs Capabilities - GeoIP";
  }
```

6. Add reference for egress-action-capa.

=> [PAUL] I added a reference to the egress-action-capa.

OLD:

```
identity egress-action-capa {
    description
      "Base identity for egress action";
}
```

NEW:

```
identity egress-action-capa {
    description
      "Base identity for egress action";
    reference
      "draft-ietf-i2nsf-capability-04: Information Model
       of NSFs Capabilities - Egress action";
  }
```

7. RFC 2460 is obsoleted by RFC 8200.

=> [PAUL] I replaced RFC 2460 with RFC 8200 as a reference.

8. Suggest hyphenation of identifiers ipv4-same-ip, ipv4-geo-ip, and ipv6-ip-opts.

=> [PAUL] I changed ipv4-geoip and ipv6-ipopts into ipv4-geo-ip and ipv6-ip-opts, respectively.

9. Suggest hyphenation of anti-virus and anti-ddos both in identifiers and in the text.

=> [PAUL] I changed antivirus and antiddos into anti-virus and anti-ddos, respectively.

10. Suggest providing definitions for absolute and periodic time.

=> [PAUL] I added the definitions for absolute and periodic time.

OLD:

Time capabilities are used to specify capabilities when to execute the I2NSF policy rule.

The time capabilities are defined as absolute time and periodic time.

NEW:

Time capabilities are used to specify capabilities when to execute the I2NSF policy rule.

The time capabilities are defined as absolute time and periodic time.

The absolute time means the exact time to start or end.

The periodic time means repeated time like day, week, or month.

11. The References do not include all the RFCs referenced by YANG model reference statements.

=> [PAUL] I added RFCs referenced by YANG model reference statements such as RFC 768, RFC 790, RFC 791, RFC 792, RFC 793, RFC 3261, and RFC 8200.

Reviewer: Carl Moberg

Review result: Almost Ready

This is my review of the ietf-i2nsf-capability@2019-03-28.yang module as part of draft-ietf-i2nsf-capability-data-model-04.

The module cleanly passes validation (i.e. 'pyang --ietf') and I have been able to load it into a NETCONF server and done basic operations on it (add, query for and remove capabilties).

I have one high-level concern and a couple of nits.

This document defines "a YANG data model for capabilities of various Network Security Functions (NSFs)". After my initial reading of the draft and I2RS background material I found it hard to understand which of the components in the I2RS reference architecture that would implement the YANG module (i.e. provide NETCONF or RESTCONF protocol implementations). The draft says the following:

“This document provides a data model using YANG [RFC6020][RFC7950] that defines the capabilities of NSFs to centrally manage capabilities of those security devices. The security devices can register their own capabilities into Network Operator Management (Mgmt) Systems (i.e., Security Controllers) with this YANG data model through the registration interface

[RFC8329].”

This seems to point in the direction of the 'Network Operator Managemen (Mgmt) Systems' as the location of the YANG datastore, i.e. where this module would be implemented.

My main question then becomes; given the fact that the top-level element of the data model is a container ('nsf') with a set of leaf-lists and containers under it, this model seems to only allow for the registration of one (1) single NSF. This seems to be also supported by the language of the description clauses referencing "network service function" in singular.

I would intuitively expect such a registry to be able to store the capabilities of a multitude of NSFs. I would appreciate if the authors could clarify the intent and expected usage of the model based on this question.

OLD:

```
module: ietf-i2nsf-capability
  +--rw nsf
     +--rw time-capabilities*                    enumeration
     +--rw event-capabilities
     |  …
```

NEW:

```
module: ietf-i2nsf-capability
  +--rw nsf* [nsf-name]
     +--rw nsf-name              string
     +--rw time-capabilities*                    enumeration
     +--rw event-capabilities
     |  …
```

Given my initial struggles I would suggest adding clearer upfront language on the location of the module and the addition of usage examples of e.g. NSFs registering capability instances to registry. (See https://tools.ietf.org/html/rfc8407#section-3.12). I believe that would provide additional and helpful context to the usage of the model.

=> [PAUL] I added the XML examples according to your comments in the Section Appendix A. Configuration Examples.

The following drafts are referenced in 'reference' and 'description' fields in the YANG module, but are missing from the Informative References section of the draft. (See https://tools.ietf.org/html/rfc8407#appendix-A.) - draft-hong-i2nsf-nsf-monitoring-data-model-06 - draft-ietf-i2nsf-capability-04 - draft-dong-i2nsf-asf-config-01

=> [PAUL] I added draft-ietf-i2nsf-nsf-monitoring-data-model-01, draft-ietf-i2nsf-capability-04, and draft-dong-i2nsf-asf-config-01.

The modules consistently seem to spell out 'capabilities', but shorten 'capability' to 'capa', e.g.:

+--rw condition-capabilities

| +--rw generic-nsf-capabilities

| | +--rw ipv4-capa* identityref

I would suggest following https://tools.ietf.org/html/rfc8407#section-4.3.1 and spell out 'capability' unless the authors are of the opinion that 'capa' is a well known abbreviation.

=> [PAUL] I changed “capa” into “capability”.

Remove the following references (they're not used):

[RFC6087] Bierman, A., "Guidelines for Authors and Reviewers of YANG Data Model Documents", RFC 6087, DOI 10.17487/RFC6087, January 2011, <https://www.rfc-editor.org/info/rfc6087>.

[RFC6991] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6991, DOI 10.17487/RFC6991, July 2013, <https://www.rfc-editor.org/info/rfc6991>.

=> [PAUL] I deleted RFC 6087 and RFC 6991 from the references.

The format used to reference drafts vary in format, some use the 'ietf-draft' prefix in the reference (e.g. '[draft-ietf-i2nsf-sdn-ipsec-flow-protection]') and some don't (e.g. '[i2nsf-advanced-nsf-dm]')

=> [PAUL] We unified the format for references such as ‘ietf-draft’ prefix.

Oh. and it looks like the email address of the WG Chair (no less! :-) is spelled incorrectly:

=> [PAUL] I revised the email address of the WG Chair.

Thanks.

Best Regards,

Paul Jeong