Operations and Management Area Working Group
Internet-Draft
Intended status: Informational
Expires: 3 April 2025

F. Hu
D. Hong
China Southern Power Grid
L. Xia
Huawei Technologies

30 September 2024

A YANG Data Model for Network Element Threat Surface Management

draft-hu-opsawg-network-element-tsm-yang-00

Abstract

This document defines a base YANG data model for network element threat surface management that is application- and technology-agnostic.

Commenté [MB1]: I have troubles to digest this given the technology-specific listed in the main document.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

With more and more advanced ~~network~~ attacks on network infrastructures, one important ~~thing~~ aspect of network device security management is to increase the security visibility and observability overall. To achieve this, on the one hand, the device normal security posture should be defined in advance, so that ~~the~~ an abnormal security status or operation of the device can be identified in a timely manner. On the other hand, from the attacker perspective, how to comprehensively define the threat surface of a device, and manage potential risks through timely monitoring is becoming vital.

Network element threat surface management has a similar concept as External Attack Surface Management (EASM) which is ~~defines~~ defined as "refers to the processes, technology and managed services deployed to discover internet-facing enterprise assets and systems and associated exposures which include misconfigured public cloud services and servers, exposed enterprise data such as credentials and third-party partner software code vulnerabilities that could be exploited by adversaries.". Comparing with EASM as a larger system and methodology, this document presents a specific implementation for network device threat surface management. Furthermore, the difference between the threat surface and attack surface is clarified briefly here: ~~The~~ an threat surface may not have vulnerabilities or be an attack surface. However, it is exposed to the attackers and faces threats from them. Therefore, its security risk is high. However, ~~the~~ an attack surface can be accessed by attackers and has vulnerabilities~~,~~; that is, it is both exposed and vulnerable, and the security risk is very high. In summary, not all threat surfaces will become attack surfaces, only exploitable threat surfaces with corresponding attack vectors will become an attack surface.

Commenté [MB2]: Add a reference

Commenté [MB3]: I don't get. This is still a risk + can be used to mount attacks.

In the past, the IETF has existing work about security posture definition, collection, and assessment, including the concluded Network Endpoint Assessment (NEA) and Security Automation and

Continuous Monitoring (SACM) working groups [RFC5209][RFC8248]. They have mainly finished the standard definition of general use cases and requirements, architecture and communication protocols, and software inventory attribute definition and so on. Recently, the extended MUD YANG model for SBOM and vulnerability information of devices defined in [RFC9472], and the extended MUD YANG model for (D)TLS profiles for IoT devices proposed in [I-D.ietf-opsawg-mud-tls], are all aiming to propose the specific security posture model definition. Similarly, this document proposes the device threat surface YANG model.

a mis en forme : Surlignage

Section 2 ~~of this document~~ defines the basic framework of the threat surface management.

Based on the above definitions, Section 3 ~~of this document~~ defines the YANG model for the device threat surface management.

1.1. Terminology and Notations

The following terms are defined in [RFC7950] and are not redefined here:

- client
- server
- augment
- data model
- data node

The following terms are defined in [RFC6241] and are not redefined here:

- configuration data
- state data

The terminology for describing YANG data models is found in [RFC7950].

Following terms are used for the representation of the hierarchies in ~~the~~ a network inventory.

Network Element:

a manageable network entity that contains hardware and software units, e.g., a network device installed on one or several chassis.

Chassis:

a holder of the device installation.

Slot:

a holder of the board.

Component:

a unit of the network element, e.g. hardware components like chassis, card, port, software components like software-patch, bios, and boot-loader.

Board/Card:

a pluggable equipment can be inserted into one or several slots/ sub-slots and can afford a specific transmission function independently.

Port:

an interface on board

1.2. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.3. Tree Diagram

The meaning of the symbols in this diagram is defined in [RFC8340].

1.4. Prefix in Data Node Names

In this document, names of data nodes and other data model objects are prefixed using the standard prefix associated with the corresponding YANG imported modules, as shown in ~~the following t~~Table 1.

Prefix	Yang Module	Reference
inet	ietf-inet-types	[RFC6991]
yang	ietf-yang-types	[RFC6991]
ianahw	iana-hardware	[IANA_YANG]
ni	ietf-network-inventory	RFC XXXX

Table 1: Prefixes and corresponding YANG modules

RFC Editor Note: Please replace XXXX with the RFC number assigned to this document. Please remove this note.

Commenté [MB4]: I guess you meant assigned to the IVY ietf-network-inventory document.

2. Definition of Threat Surface

2.1. Overview

Figure 1 depicts the overall framework of the network element threat surface management:

```
                   +------------------+
                   |  Threat Surface  |
                   +--------+---------+
                            |
         +-------------+----+-------+------------+
         |             |            |            |
         |             |            |            |
         |             |            |            |
         |             |            |            |
    +----v----+  +-----v---+  +-----v---+ +------v------+
    |Interface|  | Service |  | Account | | Version &   |
    |Exposure |  |Exposure |  |Exposure | |Vulnerability|
    +---------+  +---------+  +---------+ +-------------+
```

Figure 1: Network Element Threat Surface Management Framework

Commenté [MB5]: What is the source of this framework?

2.2. Interface Exposure

Device interfaces include physical interfaces (such as Gigabit Ethernet interfaces) and logical interfaces (such as POS, tunnel, and loopback), and IP management layer interfaces for local access.

a mis en forme : Surlignage

Interface exposure is classified as follows:

* Unused Interfaces:

  - Definition: The physical status of the interface is Down, but the administrative status is not shutdown.

  - Recommended security hardening operation: Set the interface management status to shutdown.

* IP interface exposure:

  - Definition: The interface has the IP (including primary and secondary IP addresses) configured for local access.

  - Recommended security hardening operation: If the address does not have service requirements, delete the management interface. Otherwise, check and set the corresponding access control policy, such as ACL, is configured.

With the existing definitions of "A YANG Data Model for Interface Management" [RFC8343] and "A YANG Data Model for IP Management" [RFC8344], the interface exposure information can be retrieved with NETCONF [RFC6241] Subtree Filtering mechanism as following example:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get-data xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-nmda"
            xmlns:ds="urn:ietf:params:xml:ns:yang:ietf-datastores">
    <datastore>ds:operational</datastore>
    <subtree-filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name/>
          <type/>
          <enabled/>
          <oper-status/>
```

```
            <admin-status/>
            <if-index/>
            <phys-address/>
                   <ipv4>
                   <address/>
                   </ipv4>
                   <ipv6>
                   <address/>
                   </ipv6>
          </interface>
        </interfaces>
      </subtree-filter>
    </get-data>
  </rpc>
```

In addition, the realtime change of the above information can be notified on time with NETCONF pub/sub mechanisms [RFC8639][RFC8640][RFC8641] as following examples:

```
<netconf:rpc xmlns:netconf="urn:ietf:params:xml:ns:netconf:base:1.0"
             message-id="101">
  <establish-subscription
    xmlns="urn:ietf:params:xml:ns:yang:ietf-subscribed-notifications"
    xmlns:yp="urn:ietf:params:xml:ns:yang:ietf-yang-push">
    <yp:datastore xmlns:ds="urn:ietf:params:xml:ns:yang:ietf-datastores">
      ds:operational
    </yp:datastore>
    <yp:datastore-subtree-filter>
      <interfaces xmlns="urn:ietf:params:xml:ns:yang:ietf-interfaces">
        <interface>
          <name/>
          <type/>
          <enabled/>
          <oper-status/>
          <admin-status/>
          <if-index/>
          <phys-address/>
                  <ipv4>
                   <address/>
                  </ipv4>
                  <ipv6>
                   <address/>
                  </ipv6>
        </interface>
      </interfaces>
      </interfaces>
    </yp:datastore-subtree-filter>
    <yp:on-change/>
  </establish-subscription>
</netconf:rpc>
```

2.3. Service Exposure

Here, services refer to the corresponding protocols running on devices, including SNMP, FTP, Telnet, SSH, TFTP, NTP, RADIUS, TACACS, SYSLOG, PORTAL, NETCONF, RESTCONF, SFTP, HTTP, HTTPS, and RPC.

Commenté [MB6]: How this ones were selected?

Service exposure is classified as follows:

- Insecure protocols:

  - Definition: The protocol used by the service is insecure, such as Telnet and SNMPv2.

  - Recommended security hardening operation: Disable the service or replace the protocol with a secure one, for example, replace Telnet with SSH.

- Abnormal service IP address:

  - Definition: The service binding IP address is invalid or is not within the predefined management address range.

  - Recommended security hardening operation: Change the IP address bound to the service to a valid address and set the corresponding security policy.

- Weak service security configuration:

  - Definition: The security configuration of the corresponding service is insufficient. For example, weak algorithms or passwords are used, or ACLs are not configured.

  - Recommended security hardening operation: Modify all weak security configurations.

- Abnormal Service port:

  - Definition: It is found that the service uses an invalid, incorrect, or redundant port, or there is a port that cannot correspond to the service.

  - Recommended security hardening operations: Reconfigure all incorrect ports and disable invalid and redundant ports.

2.4. Account Exposure

To add.

2.5. Version and Vulnerability

The software version and vulnerability information directly affect the device threat surface. The any above threat surface may have specific problems in a specific version. The problems may be caused by the device itself or the third-party open-source implementation.

With the existing definitions of “A YANG Data Model for Network Inventory” [I-D.ietf-ivy-network-inventory-yang], the version and vulnerability information can be retrieved with NETCONF [RFC6241] Subtree Filtering mechanism as following example:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <get-data xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-nmda"
            xmlns:ds="urn:ietf:params:xml:ns:yang:ietf-datastores">
    <datastore>ds:operational</datastore>
    <subtree-filter>
      <network-inventory
            xmlns="urn:ietf:params:xml:ns:yang:ietf-network-inventory">
        <network-elements>
          <network-element>
            <ne-id/>
            <ne-type/>
            <name/>
            <hardware-rev/>
            <software-rev/>
            <software-patch-rev/>
            <product-name/>
            <components>
              <component>
                <component-id/>
                <name/>
                <hardware-rev/>
                <software-rev/>
                <software-patch-rev/>
                <product-name/>
              </component>
            </components>
          </network-element>
        </network-elements>
      </network-inventory>
    </subtree-filter>
  </get-data>
</rpc>
```

3. YANG Data Model for Network Element Threat Surface Management

To add.

4. Manageability Considerations

<Add any manageability considerations>

5. Security Considerations

<Add any security considerations>

6. IANA Considerations

<Add any IANA considerations>

7. References

7.1. Normative References

[IANA_YANG]
IANA, "YANG Parameters", n.d., <https://www.iana.org/assignments/yang-parameters>.

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and

Requirements", RFC 5209, DOI 10.17487/RFC5209, June 2008, <https://www.rfc-editor.org/info/rfc5209>.

[RFC8248] Cam-Winget, N. and L. Lorenzin, "Security Automation and Continuous Monitoring (SACM) Requirements", RFC 8248, DOI 10.17487/RFC8248, September 2017, <https://www.rfc-editor.org/info/rfc8248>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8340] Bjorklund, M. and L. Berger, Ed., "YANG Tree Diagrams", BCP 215, RFC 8340, DOI 10.17487/RFC8340, March 2018, <https://www.rfc-editor.org/info/rfc8340>.

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