The Data Model of Network Infrastructure Device Data Plane Security Baseline

draft-xia-sacm-nid-dp-security-baseline-03

Liang Xia                 Huawei Technologies
Guangyin Zheng           Huawei Technologies
Wei Pan                  Huawei Technologies

IETF 103, Bangkok
Quick Recap

• **Objective**
  Define a minimum set of configuration and status parameters of the security related functions/services on a network device that can be collected by SACM collector and further consumed by SACM evaluator to benchmark the device security postures.

• **Security Baseline Overview**

  ![Security Baseline Diagram]

  - **App. Layer**
    - Web app security
    - Sensitive data encryption
    - Privacy protection
    - Secure third-party components
  
  - **Network Layer**
    - CTRL. Plane
      - Protect control plane signaling exchange against eavesdropping, tampering, forging, and flooding attacks
    - Data Plane
      - Protect data plane traffic against eavesdropping, tampering, forging, and flooding attacks
  
  - **Infra. Layer**
    - MGT. Plane
      - Protect network OAM process and management platform against various attacks
    - The fundamental security functions to secure the device itself.
    - The security functions provided by the device to upper layer apps.
Updates to -03 version

• Data Module Structure
  ✓ Re-organize the data module structure of the security functions in a classified way, example as follows

```
module: layer2-protection
  +--rw mac-limit
      +--rw vlan-mac-limit
      +--rw interface-mac-limit
      ...
  +--rw traffic-suppress
      +--rw vlan-traffic-suppress
      +--rw interface-traffic-suppress
      ...
```
Example 1: Layer2 Protection

• The difference of the brief structure between before and after is as below:

Before

module: mac-limit
   +--rw mac-limit
      +--rw vlan-mac-limit
      +--rw interface-mac-limit
      ...
   +--rw vlan-traffic-suppress
   +--rw interface-traffic-suppress
   ...

After

module: layer2-protection
   +--rw mac-limit
      +--rw vlan-mac-limit
      +--rw interface-mac-limit
      ...
   +--rw traffic-suppress
      +--rw vlan-traffic-suppress
      +--rw interface-traffic-suppress
      ...

Example 2: DHCP Snooping

• The difference of the brief structure between before and after is as below:

Before

module: dhcp-snooping
  +--rw dhcp-snp-global
    +--rw enable
    +--rw packet-check
    +--rw rate-limit
    ...
  +--rw dhcp-snp-vlan
    +--rw enable
    +--rw packet-check
    +--rw rate-limit
    ...
  +--rw dhcp-snp-interface
    +--rw enable
    +--rw packet-check
    +--rw rate-limit
    ...

After

module: dhcp-snooping
  +--rw dhcp-snp-global
    +--rw enable
    +--rw packet-check
    +--rw rate-limit
    ...
  +--rw dhcp-snp-vlan
    +--rw enable
    +--rw packet-check
    +--rw rate-limit
    ...
  +--rw dhcp-snp-interface
    +--rw enable
    +--rw packet-check
    +--rw rate-limit
    ...
  +--rw dhcp-snp-rate-limit
    +--rw global
    +--rw vlan-config
    +--rw interface-config
    ...

Future work

• Continue optimizing the data model

• Complete the YANG modules for all data plane baseline blocks.

• Seek more comments and co-authors are welcome