Data Plane Security Baseline Data Model for Network Infrastructure Device

draft-xia-sacm-nid-dp-security-baseline-00

Liang Xia Huawei
Guangying Zheng Huawei
Yue Dong Huawei

IETF-101, London
March 22, 2018

Agenda

- Motivation
- Draft Overview
- Data Model Design Principles
- Updates in -01 version
- Overlapping Analysis with Existing YANG Models
- Next Steps and Plans

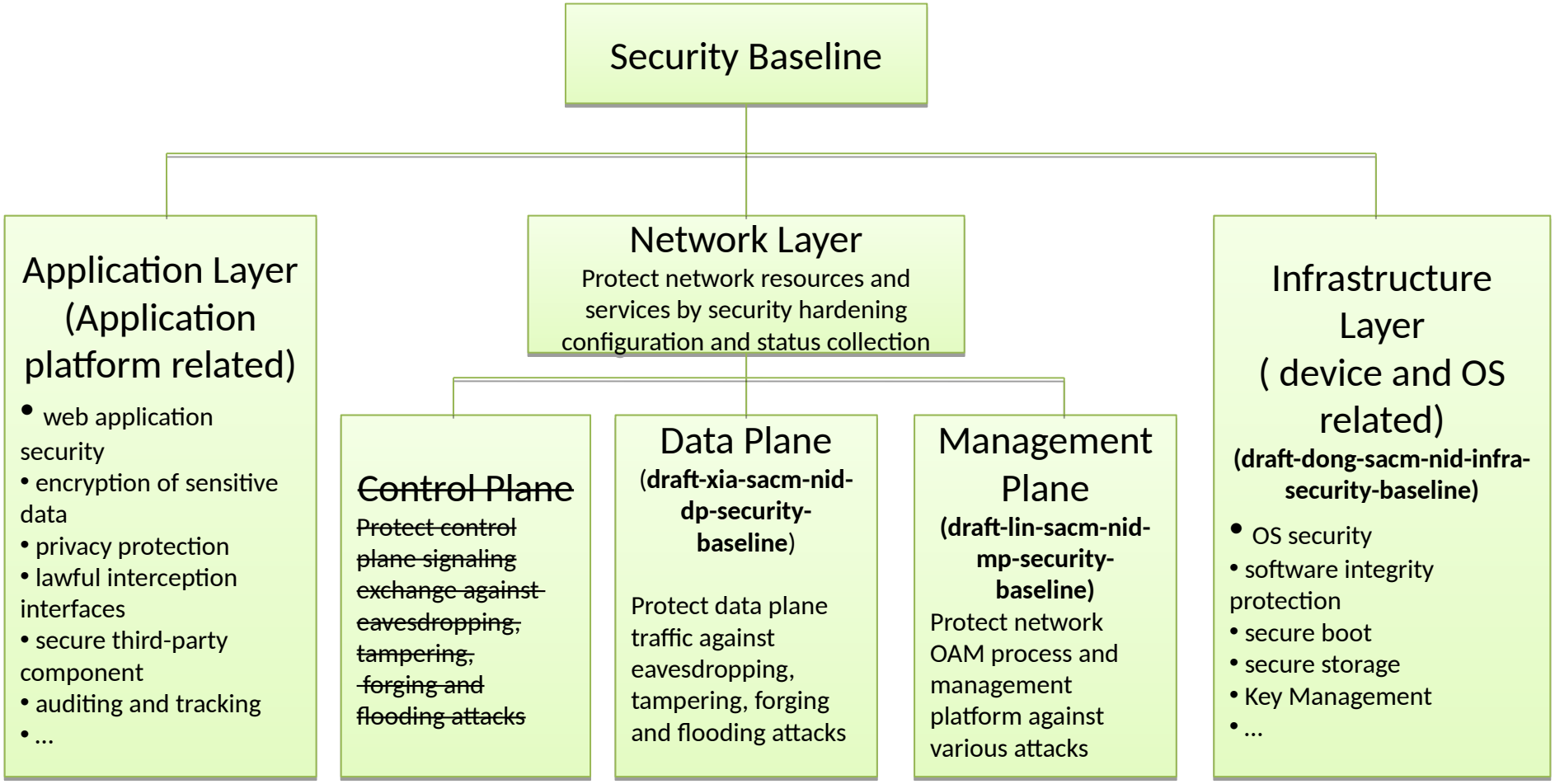
Motivation

- PANIC (The Posture Assessment Through Network Information Collection):
  - natural extension of current SACM to cover network infrastructure devices (i.e., router, switch, FW, etc): *draft-waltermire-panic-scope-02*
  - collect security posture for assessment: asset, software, **vulnerability**, and **configuration**…
- SACM re-charter:
  - Collection, Evaluation and Messaging

Draft Overview … (1/2)

- Security situatioin for network infrastructure devices
  - unsafe access channels: telnet, SNMP v1/v2
  - TCP/IP network openness
  - Network and device complexity results in more security challenges
  - Capability mismatch between data plane and control plane
- Objectives of network infrastructure device's "security baseli ne"
  - Identify threats and vulnerabilities of devices: unnecessary service s, insecure configurations, abnormal status…
  - enforce the security hardening measurements: update patching, m odify the security configuration, enhance the security mechanism …

Draft Overview … (2/2)



Data Model Design Principles

- Several design principles:
  - A Minimal but essential set of security baseline information
  - Build on the mature work in IETF:
    - YANG push and sub/pub mechanisms, and YANG model
    - Brokering YANG push telemetry into SACM statements (align with SACM IM) using mechanisms like: [I-D.ietf-birkholz-sacm-yang-content]
    - Publish SACM statement via xmpp-grid, or others…
  - Avoid overlapping with existing YANG models
    - Search https://yangcatalog.org/, and all IETF YANG drafts
    - Thanks Kathleen and Nancy for pointing out this issue ^--^

Data Plane YANG Model

updates of draft-xia-sacm-nid-dp-security-baseline-01

In general, two major updates:

1. Lots of editorial nits;
2. Largely simply the data model (58 pages to 44 pages) by:
    1) Reusing the existing DMs and augmenting them;
    2) Merging and consolidating overlapping contents

More specific:

- **L2-protection**
  - Mac-limit-control
  - BUM-suppression
- **ARP-protection**
  - ARP-anti-spoofing
  - ARP-anti-flooding
- **URPF (Unicast Reverse Path Forwarding)**

  Simplify the DM by reusing classifier definition in the draft-asechoud-rtgwg-qos-model-04 and augmenting it
- **DHCP-Snooping**

  dhcp snooping trusted interface, dhcp snooping check, dhcp snooping bind-table, dhcp snooping max-user-number and dhcp snooping alarm user-limit …
- **CPU-protection (Merging the control-plane-protection and the data-plane-protection)**
  - Protocol traffic protection: Matching and Grouping traffics into different queues (black/white/user-defined list, …), CPU CAR and queues scheduling, alarms, protocol control, counting…
  - Host CAR
- **TCP/IP-attack-defense**

  malformed packets, fragmented packets, TCP SYN packets, and UDP packets

Control Plane YANG Model
draft-dong-sacm-nid-cp-security-baseline-00

- BGP
  - Resource Public Key Infrastructure (RPKI), this YANG data model has been proposed in another draft (**draft-zhdankin0idr-bgp-cfg-00**)
  - BGP authentication
- OSPF
  - OSPF authentication, the OSPF authentication YANG data model has already been proposed in another draft (**draft-ietf-ospf-yang-09**) in netmod WG.
- ISIS
  - Checksum
  - ISIS authentication, the ISIS authentication YANG module has already been proposed in another draft (**draft-ietf-isis-yang-isis-cfg-18**).
- MPLS
  - LDP authentication, the LDP authentication YANG module has already been proposed in another draft (**draft-ietf-mpls-ldp-yang-02**)
  - RSVP authentication, the RSVP authentication YANG module has already been proposed in another draft (**draft-ietf-teas-yang-rsvp-07**)
- Keychain

  [RFC 8177] YANG Data Model for Keychain
- GTSM
  - GTSM for BGP, OSPF, MPLS-LDP, RIP

  The MPLS-LDP and OSPF YANG modules have already included the GTSM configuration, but the BGP and RIP GTSM configuration haven't been in any other drafts.

Net Steps and Plans

- keep on refinement
  - Simplify current security baseline data model
  - Consider about: event stream, configuration upd ate, filter…
  - Combination with SACM information model: TE a ttributes, guidance, evaluation results…
  - Other essential security baselines: application lay er
- Welcome comments and co-authors

Thanks!

Liang Xia (Frank)