Security Baseline Data Model for Network Infrastructure Device

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

Liang Xia Huawei

Guangying Zheng Huawei

Yue Dong Huawei

IETF-100, Singapore
Nov 15, 2017

Agenda

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

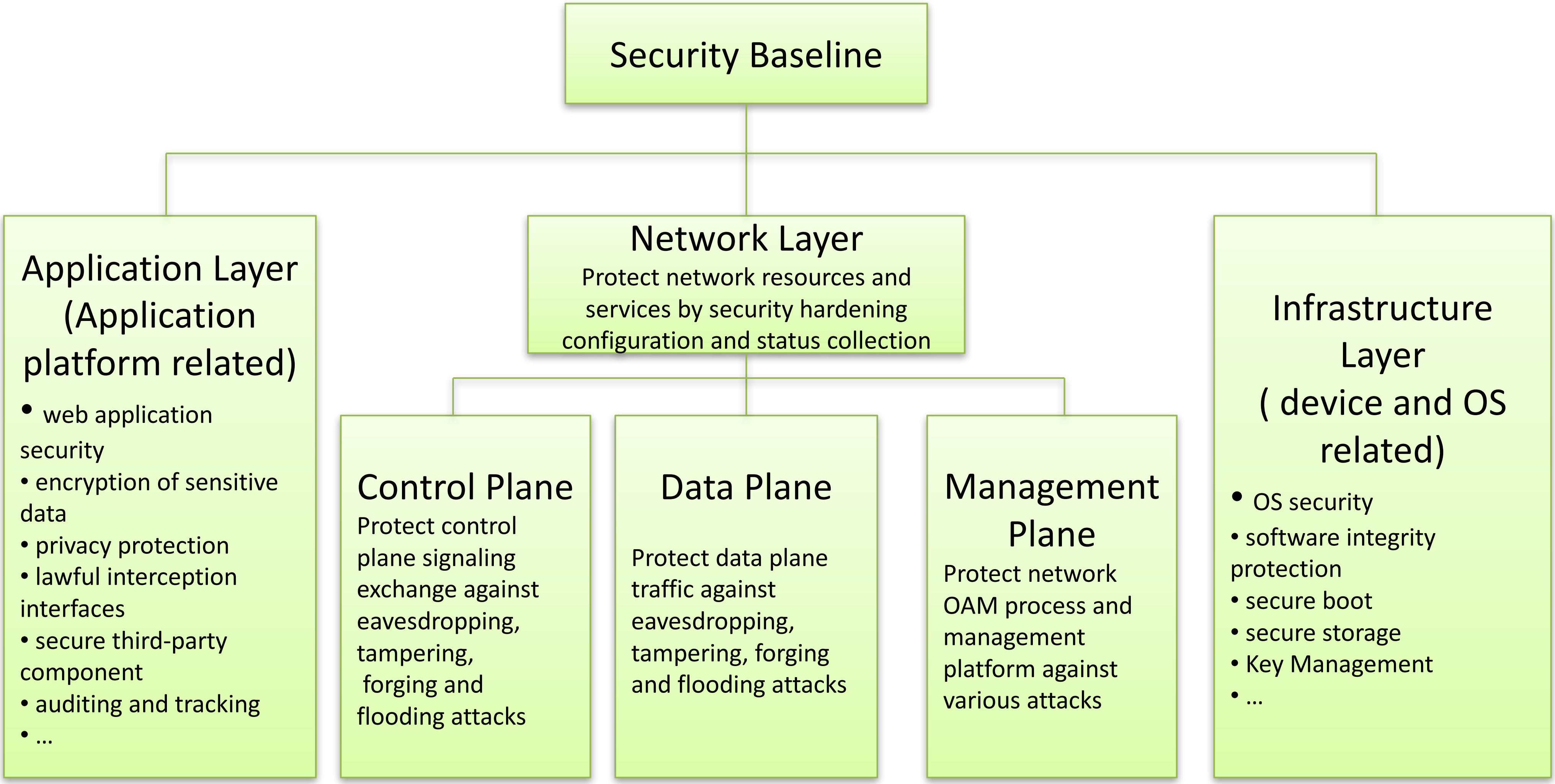
Motivation

- 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 circumstances 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 baseline"
  - Identify threats and vulnerabilities of devices: unnecessary services, insecure configurations, abnormal status…
  - enforce the security hardening measurements: update patching, modify the security configuration, enhance the security mechanism…

Draft Overview … (2/2)



Security Baseline

Application Layer (Application platform related)

- web application security
- encryption of sensitive data
- privacy protection
- lawful interception interfaces
- secure third-party component
- auditing and tracking
- …

Network Layer

Protect network resources and services by security hardening configuration and status collection

Control 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

Management Plane

Protect network OAM process and management platform against various attacks

Infrastructure Layer (device and OS related)

- OS security
- software integrity protection
- secure boot
- secure storage
- Key Management
- …

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

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

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

  dhcp snooping trusted interface, dhcp snooping check, dhcp snooping bind-table, dhcp snooping max-user-number and dhcp snooping alarm user-limit …
- **Control-Plane-protection**

  Host defend by protocol type, Host defend by 5-tuple, HostCaptPkt
- **Data-Plane-protection**

  CPU car, packet statistic, Attack source, QPktStat, CAR configuration, Attackoutput, AccessUserStat, CapturePacket…
- **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 update, filter…
  - Combination with SACM information model: TE attributes, guidance, evaluation results…
  - Other essential security baselines
- Welcome comments and co-authors

Thanks!

Liang Xia (Frank)