The Data Model of Network Infrastructure Device Security Baseline

draft-dong-sacm-nid-infra-security-baseline-00

Yue Dong Huawei

Liang Xia Huawei

Contents

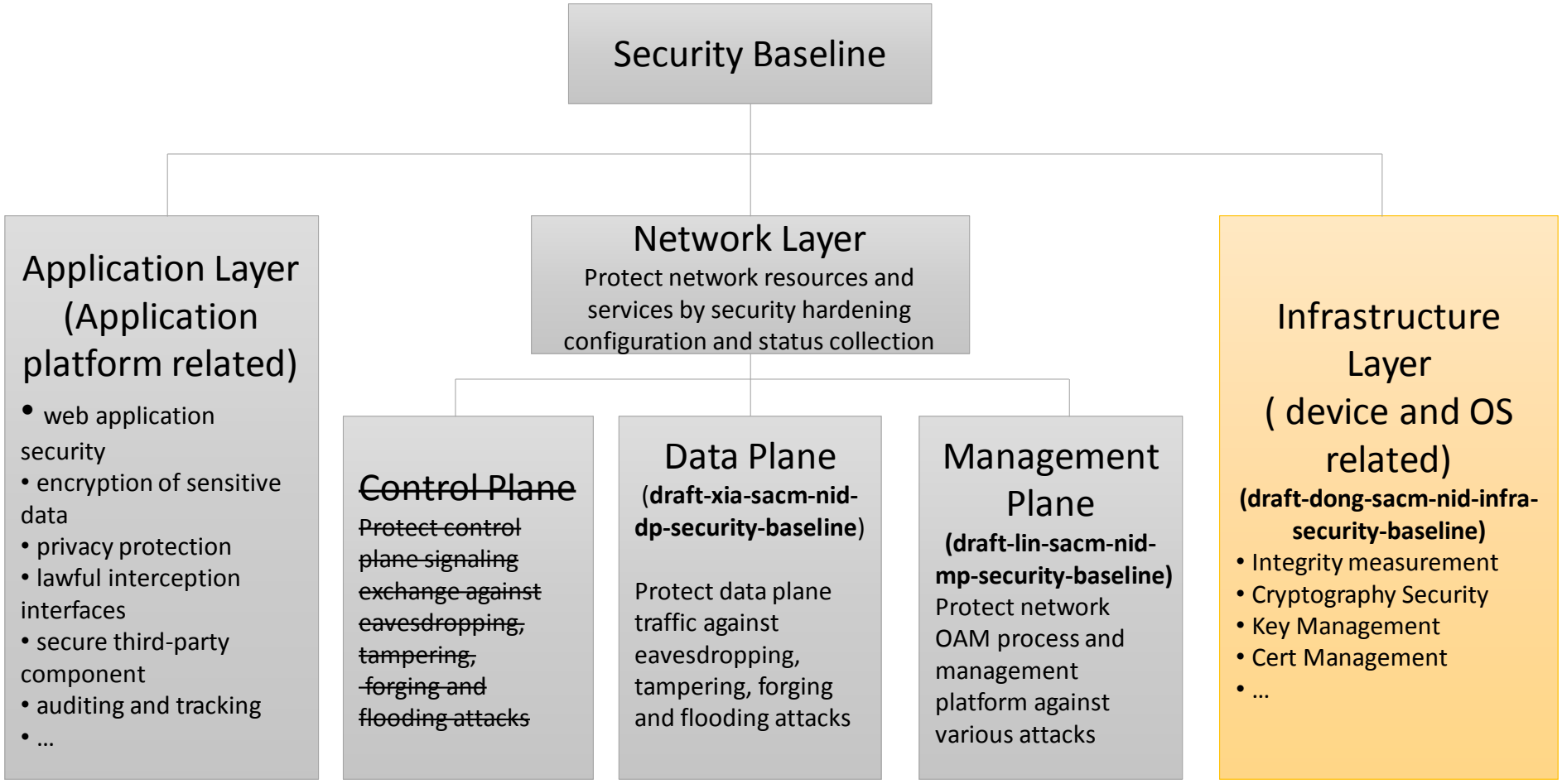
- Objectives
- Security Baseline Overview
- Infra. Layer Security Baseline
- Next Step

Objectives

- Define a minimum set of network device infrastructure layer security attributes (configuration and status parameters) that can be collected by the SACM collector and further consumed by the SACM evaluator to benchmark the device security postures.

Security Baseline Overview

- ***Infrastructure Layer***
  - The fundamental security functions about the device itself,
  - The security functions that provided by the device to the upper layer applications.



Infra. Layer Security Baseline Design

- Integrity measurement
  - Root of trust
  - Cryptography engine: supported cryptographic algorithms
  - Trust measurement: bootstrapping, software update
- Cryptography security
  - Symmetrical cryptography: block cipher, stream cipher
  - Asymmetrical cryptography: asymmetrical encryption, digital signature
  - Hash functions
  - Message authentication code
  - Key derivation function
  - Random number generator
- Key management
  - The configuration and status parameters to ensure the key (pairs) are security enough in its entire lifecycle (i.e. generation, distribution, storage, update, backup, destroy, and etc.)
- Cert management
  - Cert management: Request, update, validate, cert info
  - CRL management: CRL update

Next Step

- Complete the infrastructure layer data model.
- How the defined data model can be consumed existing protocols, such as YANG push?
- Maybe how the selected attributes/postures in the data model can be evaluated?

- Comments and co-authors are warmly welcome!