Data model of Security Baseline for Network Infrastructure Device

draft-xia-sacm-nid-dp-security-baseline-02

draft-dong-scam-nid-infra-security-baseline-01

Liang Xia	Huawei Technologies
Guangyin Zheng	Huawei Technologies
Yue Dong	Huawei Technologies

IETF 102, Montreal

July 2018

Agenda

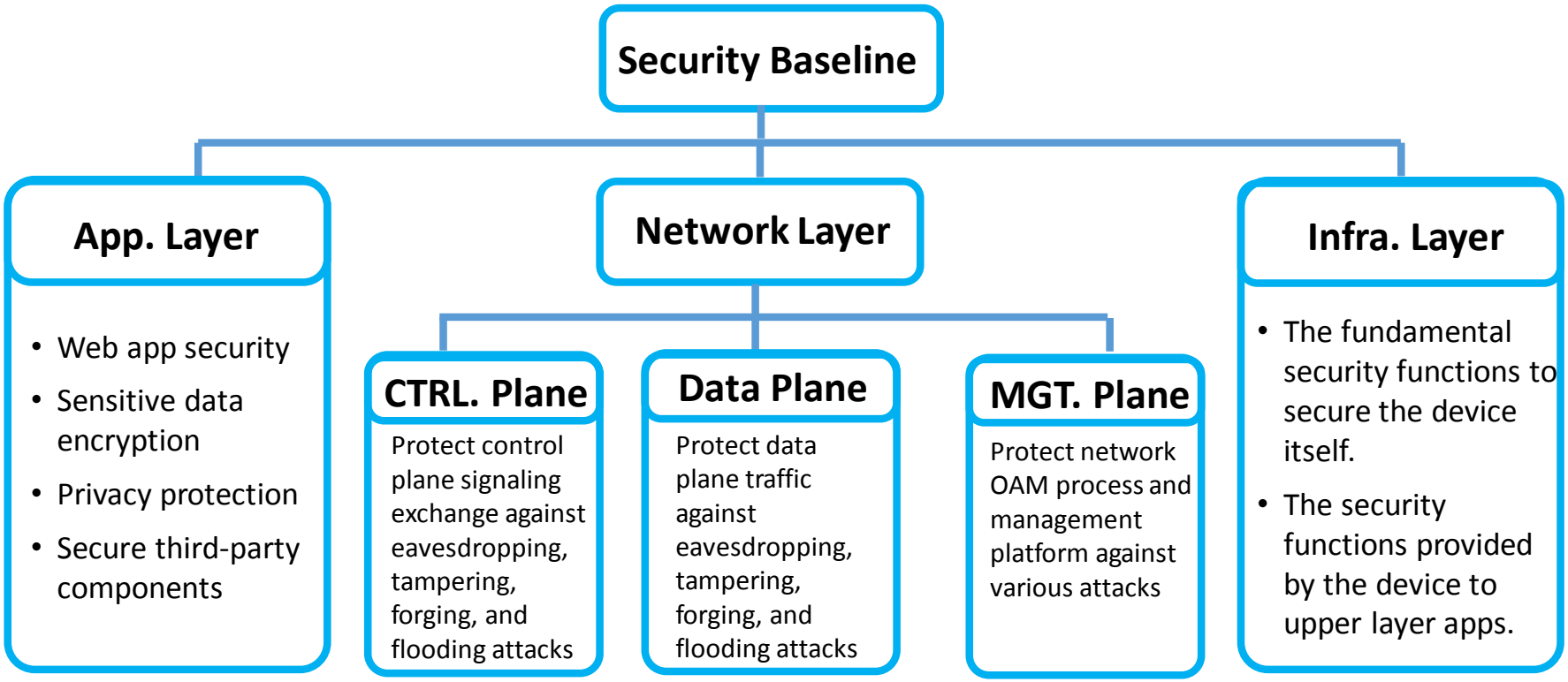
- Recap of Objective and Classification of Security Baseline
- Data plane security baseline draft updates
- Infra. layer security baseline draft updates
  - ✓Integrity measurement
  - ✓Cryptographic algorithms
  - ✓Key management

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



Data plane draft updates to -02 version

- The configuration attributes for VSI broadcast traffic suppression function are added in the L2-protection;
- The naming rules for all statements in tree diagram and YANG modules are changed;

  e.g. macLimitRules → mac-limit-rules
- More derived data typed are added into the YANG module;

  e.g. mac-type, suppress-type, limit-type, etc.
- YANG module passed the YANG validate.

Infra. layer updates overview

- Introduction

  Rewrote the introduction part to make the motivation and the structure of the draft more clear

- Data Model

  Optimize the data model by

  - Delete the redundancy parts
  - Give up to collect the confidential information such as: private key, initial vector, and etc.

- YANG Module

  Complete the yang modules for integrity measurement and the groupings of the cryptographic algorithms

Integrity measurement updates

- Delete the key store information (e.g. key code, key store, key lifetime, and etc.). This is already covered in a separate key management module. And the private key should be keep confidential.
- Delete the crypto engine container. This part has already covered in the cryptography algorithm module.

Cryptography algorithms updates

- Using groupings instead of containers, so that other modules can reference the algorithms directly;
- Put block cipher and stream cipher into a single symmetric algorithm grouping;
- DSA, ECDSA configuration attributes are added in the signature algorithm grouping;
- DH and ECDH configuration attributes are added in the key exchange groupings;
- CMAC configuration attributes are added in the message authentication code grouping.

Key management updates

- reference pre-defined algorithm groupings rather than specify the algorithms configuration details again.

Example:

Before

```
submodule: key-generation
       +--rw key-generation
          +--: (random-number-generator)
          |  +--rw generator-type                identityref
          +--: (key-derivation-function)
          |  +--rw hash-algorithm                identityref
          |  +--rw entered-password              string
          |  +--rw salt-value                    string
          |  +--rw liter-count                   int
          +--: (key-exchange)
             +--rw key-exchange-protocol         identityref
```

After

```
submodule: key-generation
       +--rw key-generation
          +--: (random-number-generator)
          |  +--rw key-randomness          decimal64
          +--: (key-derivation-function)
          |  +---u key-derivation-function
          +--: (key-exchange)
             +--rw cert-name                  string
             +---u key-exchange
```

Future work

- Continue optimize the data model
- Complete the YANG modules for all data plane baseline blocks.
- Seek more comments and co-authors are welcome

Network Infrastructure Device Management Plane Security Baseline

https://datatracker.ietf.org/doc/draft-lin-sacm-nid-mp-security-baseline/

Qiushi Lin
Liang Xia
Henk Birkholz

IETF 102

Recap

- Provide security baseline for network infrastructure devices management plane, represented by YANG data model
- Corresponding values can be transported between SACM components and used for network infrastructure device security evaluation
- Define a minimal set of security controls that are expected to be widely applicable to common network infrastructure devices
- Additional security controls can be defined by specific vendors

```
module: nid-management-plane-security
  +--rw admin-management-security
  |  +--rw admin-security-policy
  |  +--rw admin-login-security
  |  +--rw aaa-security
  |  +--ro admin-access-statistics
  +--rw system-management-security
  |  +--rw snmp-security
  |  +--rw netconf-security
  |  +--rw port-management-security
  +--rw log-security
  |  +--rw alert-notification
  |  +--rw log-overflow-action
  |  +--rw log-mode
  +--rw file-security
```

Updates since IETF 101

- Updated Account Management Security Part

  Refined the YANG tree, and provided YANG data model

  - admin-security-policy
    - account-security-policy: whether the security controls are enabled, account aging period, minimum length of the account name
    - pwd-security-policy: warning password expiration, notifying to change the password when it is used for the first time, whether check password complexity, etc
    - forbidden-word-rules: forbidding the use of some words in password
    - login-failed-limit: If an account login failed several times in a certain period, this account will be blocked for a certain time range
  - admin-login-security
    - Security controls on different login channels: console, vty, telnet, ssh, web
  - aaa-security
    - AAA schemes, RADIUS servers, TACACS+ servers
  - admin-access-statistics
    - Total number and the list of online administrators, IP block list

Next Steps

- Update the other three submodules and provide the corresponding YANG data model
- Call for collaboration from other vendors, discuss and refine the data model
- Adapt the data model to support the combination with YANG push mechanisms