# The Data Model of Network Infrastructure Device Security Baseline

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

Yue Dong Huawei

Liang Xia Huawei

IETF-101, London
March 22, 2018

# Contents

- Motivation and Objectives
- Draft Overview
- Infra. Layer Security Baseline
- Next Step

# Motivation and Objectives

❑Why in SACM

- Automate assessment of endpoint posture
  According to the up to date charter of SACM WG, a network device is an endpoint in the scope of SACM.
- SACM focus on ***collection***, evaluation, orchestration and communication. Two types of guidance to collectors:
  1) Which target endpoints to collect from, and
  2) What ***elements to collect*** from these target endpoints.

❑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.

# Network Device Security Baseline Overview

- Application Layer

  Web application security, local data encryption, and etc.
- Network Layer

  Data plane, control plane, and management plane
- ***Infrastructure Layer***
  - The fundamental security functions about the device itself,
  - The security functions that provided by the device to the upper layer applications as a secure environment.

# Infra. Layer Security Baseline Design

- Integrity measurement
  - Root key store
  - 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/simplify the infrastructure layer data model.
- How the defined data model can be coupled into the control plane protocol such as YANG push?
- How the selected attributes/postures in the data model can be evaluated?

- Comments and co-authors are warmly welcome!