Data Plane Security Baseline Data Model for Network Infrastructure Device
draft-xia-sacm-nid-dp-security-baseline-01

Liang Xia
Guangying Zheng
Yue Dong

Huawei
Huawei
Huawei

IETF-101, London
March 22, 2018
Agenda

• Objectives
• Draft Overview
• Data Model Design Principles
• Updates in -01 version
• Next Steps and Plans
Objectives

- Collect configuration and status parameters of security related functions/services on network devices.
- The collected parameters can be used to
  — identify threats and vulnerabilities of devices: unnecessary services, insecure configurations, abnormal status...
  — enforce the security hardening measurements: update patches, modify the security configuration, enhance the security mechanism...
Draft Overview

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
(draft-xia-sacm-nid-dp-security-baseline)
Protect data plane traffic against eavesdropping, tampering, forging and flooding attacks

Management Plane
(draft-lin-sacm-nid-mp-security-baseline)
Protect network OAM process and management platform against various attacks

Infrastructure Layer
(device and OS related)
- Integrity Measurement
- Cryptography Security
- Key Management
- Cert Measurement
- ......

Data Model Design Principles

• Several design principles:
  – A Minimal 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...
Data Plane YANG Model
updates of draft-xia-sacm-nid-dp-security-baseline-01

Updates to -01:
1. Lots of editorial nits;
2. Largely simplified the data model (58 pages to 44 pages) by:
   1) Reusing the existing DMs and augmenting them;
   2) Merging and consolidating overlapping contents
Updated Sections / sub-models (updated underlined sections):

- **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-rtgwq-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
Dropping Control Plane YANG Model
(as already covered in other IDs)
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.
Next Steps and Plans

• keep on refining
  – 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: application layer

• Seeking more comments and co-authors welcome
Thanks!