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 103

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
  - Administration security
  - System management security
  - Port management security
  - Log security
  - File security

Updates to -04 version

- Updates for all data modules:
  - Do not try to cover legacy situations (where unsafe protocols may be used), only focus on recommended protocols
- Updates for Administration Security
  - Define the password security policy as a feature
  - Due to the difference between security posture collection and device configuration, tailor some nodes of "ssh-server-grouping" and "tls-server-grouping" defined in other drafts
- Updates for System Management Security
  - Due to the difference between security posture collection and device configuration, data modules defined for SNMPv3 in RFC 7407 are reused and modified.
- Other updates
  - Update corresponding YANG modules
  - Editorial updates

Next Steps

- Update the Log Security and File Security sections, provide corresponding YANG modules
- Discuss with other vendors to refine the data model
- Comments are welcome