Network Infrastructure Device Management Plane Security Baseline


Qiushi Lin
Liang Xia
IETF 100
Motivation

• Define security baseline for network infrastructure devices, which can be further used in security posture assessment

• Focus on management plane security baseline and provide a data model

• Reuse the existing YANG models and provide additional modules or groupings for the missing parts
## Overall Structure

- **Management Plane Security Baseline**
  - User Authentication & Authorization
  - System Management Security
  - Log Security
  - File Security

### Existing YANG Models
- RFC7317: A YANG Data Model for System Management
- RFC7407: A YANG Data Model for SNMP Configuration
- I-D.ietf-netconf-tls-client-server
- I-D.ietf-netconf-ssh-client-server
- I-D.ietf-netconf-netconf-client-server
- I-D.ietf-netmod-syslog-model
- I-D.ietf-netmod-acl-model
User Authentication & Authorization

• Each type of user interface: Authentication mode & privilege level

  +--rw user-login-security
    |  +--rw (user-interface-type)
    |    |  +--: (console)
    |    |    |  ...  
    |    |  +--: (vty)
    |    |    |  ...  
    |    |  +--: (web)
    |    |    |  ...  
    +--rw aaa-user-authentication
      |  +--rw (aaa-mode)
      |    |  +--: (radius)  RADIUS server list
      |    |    |  ...  
      |    |  +--: (tacacs)  TACACS+ server list
      |    |    |  ...  
    +--rw user-profile
      +--rw user* [user-name]

• User Credentials Configuration
• Password Complexity Check

  • ACL rules (reuse) & IP block
  • Remote channel security: ssh (reuse), telnet

  • ACL rules (reuse) & IP block
  • HTTPS configuration security: tls (reuse), source port, etc.
System Management Security

---rw snmp-security
|   +--rw target* [name]
|   |   ...
|   +--rw target-params* [name]
|   |   ...
|   +--rw community* [index]
|   |   ...
|   +--rw vacm
|   |   ...
|   +--rw usm
|   |   ...
|   +--rw tsm
|   ...

---rw netconf-security
   +--rw listen {listen}?
   |   ...
   +--rw call-home {call-home}?

• Reuse the definition in RFC7407
  – Community-based Security Model for SNMPv1 and SNMPv2c
  – View-based Access Control Model and User-based Security Model for SNMPv3

• Reuse the definition in I-D.ietf-netconf-netconf-client-server
Log Security & File Security

- **Local Log Security**
- **Syslog**

```
+--rw log-security
   +--rw (log-mode)
      +--: (file)  User privilege level
         |   ...
      +--: (remote)  Syslog security (reuse)
         ...
```

- **Local File Security**
- **Remote Transfer Security**

```
+--rw file-security
   +--rw (file-operation)
      +--: (local)  Security check for patches, packages, configuration files
         |   ...
      +--: (remote-transfer)  Remote Transfer Security: FTP, SFTP, SCP, FTPS
         ...
```
Next Steps

• Refine the data model

• Combine the data model with SACM framework to assess network infrastructure device security posture

• Combine with existing YANG push and sub/pub mechanisms

• Please review and comment