A Security Geek’s Guide to SNMP, MIB modules, NETCONF & YANG modules

Ron Bonica

Dan Romascanu

IETF 80
What are these things?

- **SNMP** – A Simple Network Management Protocol that can be used to configure and retrieve variables on a device. In practice, SNMP is rarely used for configuration. Also can be used to monitor asynchronous notifications/traps.

- **MIB** – A Management Information Base that defines all data managed by SNMP.
What are these things? (bis)

- **NETCONF** – A network management protocol that can be used to configure and retrieve variables on a device. NETCONF is better suited to configuration than SNMP.
- **YANG** – Data Modeling Language for defining data managed by NETCONF. Defined in the NETMOD WG. To date, few YANG modules have been written.
Security of Management Protocols

- **SNMPv1** (historic)
  - Plain text password
  - Many users use a default password (public)
  - Can be, but rarely is run over IPSEC

- **SNMPv2** (historic)
  - Better cryptographic access control
  - Can be, but rarely is run over IPSEC

- **SNMPv3**
  - Current standard version
  - Defines full security framework
    - User-based Security Model (USM)
    - View-based Access Control Model (VACM)

- **NETCONF**
  - SSH transport – mandatory to implement
  - TLS - optional
Philosophy of MIB

• Every protocol should have a MIB module
  – Probably true
  – YANG modules may replace them in the future
• Every significant variable should be represented in MIB
  – Waste of time and money
  – Possible security vulnerability
    • If recommendations to use only SNMPv3 with authentication and privacy modes deployed and activated are not respected
• Represent things that you are likely to send notifications on or poll in MIB
  – Use CLI to access everything else
Why should a security dude care?

• Would it be easier to operate your security protocols if they sent notifications? If selected variables could be polled periodically by the NMS, without screen scraping the CLI?

• Could you tell the community about the security attributes of popular network management protocols?

• Could you tell the community about potential vulnerabilities created by non-standard usage of the network management protocols?
Security Risks Created By non-standard usage of Network Management Protocols

• If the privacy mode (encryption) is not deployed and activated, management protocol may expose sensitive information to someone snooping a LAN segment

• If strong authentication is not deployed and activated than unauthorized read or write access to sensitive data items can happen.

• Network Management traffic is easily spoofed if security is not deployed and activated