Title: HP OpenView Network Node Manager SPI for SNMPv3
Session #: 326
Speakers: Jeff Scheaffer, HP OpenView NSM
          David Reid, SNMP Research
The new HP OpenView Network Node Manager SPI for SNMPv3 supports secure SNMP and SNMP management through firewalls.

This session provides an overview and discussion of secure network management, including:

- the current Internet-Standard Management Framework;
- the security and administration features of SNMPv3;
- the technical architecture and configuration of the NNM SPI for SNMPv3;
- how to securely extend SNMP management through firewalls;
- elements of a complete solution.
The current Internet-Standard Management Framework

The security and administration features of SNMPv3
SNMP in One Slide

- Common organization structure for management information (SMI)
- One naming space for all management “objects” (MIB)
- Communications Protocol (SNMP)

Manager

Requests

Responses

Notifications

Agents

Networking Equipment

Servers

PCs

Software Applications
Features of SNMPv3: Security and Administrative Framework

• Security
  – Authentication – who is doing the communicating
  – Privacy – protection from disclosure
  – Authorization – what operations are allowed (e.g., read, write, notify)
  – Access control – what information objects can be read or written

• Administrative framework to support the above
SNMPv1/SNMPv2c **Not Secure**
Secure SNMPv3

Administrative Workstation

Attacker

Managed Device(s)

Firewall

SNMPv3 traffic

HP OV NNM with NNM SPI for SNMPv3

Managed System(s)
SNMPv3 Includes Everything in Versions 1 and 2c Plus…

• Authentication:
  User-based authentication of messages

• Privacy:
  The ability to encrypt management messages

• Authorization:
  The concept of users

• View-based access control:
  Restriction on what data may be read/written

• Administrative framework to support the above
Authentication

- The process of reliably determining the identity of the sender of a message
- Verify that the message received is the one sent
- Protects against following threats:
  - Masquerade (spoof sender)
  - Modification of information (change content)
  - Modification of message stream (timing, limited replay)
- Standard specifies MD5 and SHA1 for strong authentication
  - Private key model with localized keys
  - More than good enough for virtually all applications today
Privacy

• Protection from the unauthorized disclosure of data
• Encrypt SNMP payload for privacy
• Private key model with localized keys
• Standard specifies DES (56-bit)
• Standard is extensible for stronger cryptography
  – Triple-DES (168-bit keys)
  – AES (128, 192, and 256 bit keys)
  – … Others possible …
Authorization

• Each request is associated with a SNMPv3 “user” (system, person, or role)
• A user is a member of a group
• Mechanism to specify what each network manager (user) can do (read, write, notify)
• The management application determines how its “users” (operators) map to SNMPv3 “users”
Access Control

• Like authorization, access control is performed by group
• Every SNMPv3 “group” (and therefore every user) has three associated lists of what objects can be accessed on each device (read, write, notify)
• This is very fine grained, down to individual instances, if desired
• Simple or complex combinations
• Examples:
  – Read access to all network statistics
  – Read/write access to configure notifications (e.g., traps)
SNMPv3 Administrative Framework

• All of this configuration information is stored in Management Information Base (MIB) tables

• Administrative subsystems defined by standards
  – User-based Security Model (USM)
  – View-based Access Control Model (VACM)

• Standard supports remote configuration of:
  – Users
  – Groups
  – Views
  – Keys (generated from pass-phrases)
  – Older versions including community strings, if any
SNMPv3 Typical Deployment Scenarios

• A few “user” names are associated with management stations (e.g., ow1, nnmbldg4)
• Authentication used for all communications
• Both Authentication and Privacy used for sets
• Authentication and Privacy used for retrieval of sensitive information (e.g., routing tables)
• SNMP security configuration management is done by
  – Hand: Editing or copying over local configuration files
  – Security configuration distribution application(s) via SNMPv3 set requests
HP OpenView NNM and SNMPv3

• Desired Solution
  – Manage using familiar tools and procedures (e.g., NNM)
  – Manage using existing complementary applications
  – Manage using appropriate SNMP level
    • SNMPv1 and SNMPv2c for monitoring older devices in trusted environments
    • SNMPv3 for managing critical systems in less trusted regions
    • SNMPv3 for managing remote sites through less trusted regions
    • SNMPv3 for all configuration operations
  – Common repository for security configuration data
Security Solution

HP OpenView NNM

HP OpenView NNM SPI for SNMP v3

= Secure Management
HP OpenView

NNM SPI for SNMP v3
HP OpenView

NNM SPI for SNMPv3

• Integration was jointly developed by HP and SNMP Research
• Maps outbound SNMP requests to SNMPv3 requests sent to target agent
• Converts SNMPv3 responses from agent and sends back to NNM
• Receives notifications (traps and informs)
• Includes security configuration datastore
• Includes SNMPv3 Configuration Wizard application
HP OpenView NNM SPI for SNMPv3

- SNMPv3 SPI supporting SNMPv3 standards:
- User-based Security Model
- View-based Access Control Model
- Monitor network devices using appropriate SNMP security level: SNMPv3, SNMPv2c, or SNMPv1

- Securely manage DMZ
- Manage SNMPv1/SNMPv2c/SNMPv3 devices behind a firewall
- Securely manage multiple isolated sites over insecure Internet infrastructure
secure SNMP management through firewalls
Management challenges presented by security firewalls

- Many sites continue to depend on legacy (i.e., SNMPv1 and SNMPv2c) SNMP versions which provide no security.
- Network administrators are reluctant to allow SNMP-based management through firewalls.
  - In many sites, nearly all UDP traffic is disallowed across firewalls
  - Many SNMP agents in managed devices are not adequately configured or configurable to restrict the management information they divulge.
- Many sites disable ICMP across firewalls
HP OpenView NNM
Secure Polling Agent

• Manage securely to multiple isolated sites over insecure Internet infrastructure

• Manage SNMPv1/SNMPv2c devices behind a firewall
  – Preserve vast investment in SNMP-based management
  – Do not have to upgrade all devices inside the firewall
  – May want to upgrade to defend against threats from within

• Manage SNMPv3 devices behind a firewall that does not allow any SNMP traffic through the firewall
HP OpenView NNM Secure Polling Agent

- SNMP v3 SPI supporting SNMP v3 standards:
- User-based Security Model
- View-based Access Control Model
- Monitor network devices using appropriate SNMP security level: SNMP v3, SNMP v2c, or SNMP v1

- Securely manage DMZ
- Manage SNMP v1/SNMP v2c/SNMP v3 devices behind a firewall
- Securely manage multiple isolated sites over insecure Internet infrastructure
SNMPv3 over UDP through Firewalls

NNM plus the NNM SPI for SNMPv3

SNMPv3 / UDP through firewalls

Sun  HP  Internet Device with SNMP Agent

Linux  XP  Internet Device with SNMP Agent
Management Traffic in XML tunnel through Firewalls

HP OpenView NNM Secure Polling Agent

SNMPv1/v2/v3 over UDP locally

Internet Device with SNMP Agent

Management Information in XML over SSL over TCP through firewalls

NNM plus the NNM SPI for SNMPv3

HP OpenView NNM Secure Polling Agent

Sun

HP

Linux

XP

Internet Device with SNMP Agent
Key Elements of a Complete Solution

• Secure agents
• Secure management applications
• Administrative policies
• Configuration management of users, keys, etc
• Coexist with legacy systems
Secure Agents

• SNMPv3 agents available on most networking devices
• SNMPv3 agents available on most open operating systems and embedded real-time operating systems
• For integrated network and system management, smart agents based on SNMPv3 are available
  – Support common SNMPV3 administrative framework
  – Network monitoring
  – Host resource monitoring
  – File system monitoring
  – Critical application monitoring
  – Log file monitoring
  – Service monitoring
• More info on secure agents tomorrow at 8:30, session 325
Secure Management Applications

• HP OpenView Network Node Manager with HP OpenView NNM SPI for SNMPv3

• After initial configuration, NNM functions work transparently
  – MIB Browser
  – Node polling
  – Data collection

• Partner applications which use NNM SNMP stack will also work transparently
Administrative Policies

• Parts of an enterprise security policy include:
  – Who can see what?
  – Who can change what?
  – How are “users” defined?
  – What level of authentication?
  – What level of encryption?
  – How often are keys changed?
  – Who can change security configurations?
  – How are configurations changed/audited?
Configuration Management Issues

• Users, keys, notifications, etc. must be configured on both managers and agents
• Keys are generated from pass-phrases, pass-phrases not stored on managed devices
• Keys need to be changed periodically
• Configuration must be updated in a timely manner (e.g., deny rights to a terminated employee)
• Configuration needs to be done remotely from a security management station, using a secure and private method
Configuration Management Issues: SNMPv3 Remote Administration

- Need to configure manager platforms and agents in accordance with enterprise policies
- Can do it with “vi” or “edit” but really need something more friendly and powerful
- Security dependent on correct configurations
- Wizard and/or policy-based tools
- Configurable agents
- Configurable managers
Configuration Management Applications

- Configuration Management applications are very helpful to reduce complexity and human error
  - One agent at a time “wizard” application
  - Policy-based, multiple-target distribution application
SNMPv3 Configuration Wizard

Security Configurations

Configuration by systemAdmin on ultra101
SNMPv3 USM User to Create netReporter

Select the maximum security level for this SNMPv3 USM user:

- No Authentication or Privacy (noAuthNoPriv)
- Authentication without Privacy (authNoPriv)
- Authentication with Privacy (authPriv) (recommended)
Policy-based SNMP Configuration Management

Step 1. Define User
   Define SNMPv3 USM Users and/or SNMPv1 and SNMPv2c Communities to configure on managed devices.

Step 2. Define Group
   Define security groups and the read/write access available to group members.

Step 3. Assign User to Group
   Assign SNMPv3 Users and SNMPv1/SNMPv2c Communities to a security group.

Step 4. Define Notification Target
   Define destinations for agent traps/informs.

Step 5. Define Policy
   Build a configuration policy by selecting one or more security groups and the members and notification targets associated with the security group(s).

Define User(s) for Read/Write Management Access

Define the SNMPv3 USM User(s) to be used for reading and writing to managed devices. Use the buttons below to define a new SNMPv3 User or to modify or delete an existing SNMPv3 User.
Coexist with Legacy Systems

• Some managed systems will not have SNMPv3 agents
• Cannot upgrade all agents at once
• NNM SPI for SNMPv3 is multi-lingual, so fully supports a heterogeneous SNMPv1 / SNMPv2c / SNMPv3 agent environment
  – Old agent, old packet, old rules, old response
  – New agent, new packet, new rules, new response
• Properly handle SNMPv1 traps
• Properly handle SNMPv2c traps and informs
final comment...
Summary

- SNMPv3 provides secure management capabilities
- Secure SNMPv3 is available in today using the HP OpenView NNM SPI for SNMPv3 and SNMPv3 enabled agents
- HP OpenView Network Node Manager, the HP OpenView NNM SPI for SNMPv3, and the HP OpenView NNM Secure Polling Agent allows secure management through firewalls, even when managing SNMPv1/SNMPv2c devices
- After security credentials have been configured, operation using the NNM SPI for SNMPv3 is transparent to NNM functions
- Available today from SNMP Research. Available soon from HP.
Thank you!
HP OpenView NNM SPI for SNMPv3
HP OpenView NNM Secure Polling Agent

SNMPv3 Configuration Wizard

SNMPv3 Agent
SNMPv2c Agent
SNMPv3 Proxy Agent
Legacy Device

Outbound SNMP Request + target address
SNMP response + source address
SNMPv1/ SNMPv2c Trap or inform

HP OpenView Network Node Manager
HP OpenView Performance Insight and/or HP OpenView Operations

Other Network Management Software

datastore

HP OpenView NNM SPI for SNMPv3

Standard SNMPv1/v2c/v3 request
Standard SNMPv1/v2c/v3 response
Notifications SNMPv1 traps SNMPv2c/v3 traps and informs

HP OpenView Secure Polling Agent

Firewall(s)