Integrated Security
For SNMP-Based Management

Wes Hardaker
Sparta, Inc.
<hardaker@sparta.com>

May 24, 2004
Overview

• This will be an interactive session!  
  (Get ready to raise your hands)

• Problem Space
• Solution Space
• Operator Requirements
• Questions & Answers
SNMP Security History

• SNMPv1: None 1988
• SNMPv2c: None 1996
• SNMPv3: Yes, but... 1998
  – Secure authentication (MD5 and SHA-1)
  – Secure encryption (DES and AES [almost in RFC])

• SNMPv3 is more secure than v1/v2c
  – But operators were never asked
    “what do YOU need?”
    Thus, the results are less useful.
SNMPv3 Problems

• …, **but**: SNMPv3 users are SNMP specific
  – USM: User-based Security Model
  – Setup, user management, and Key distribution and updates are difficult using USM
  – Doesn’t use existing security infrastructures like Radius, Accounts, Kerberos, TACACS+, SSH Identities, X.509 Certificates, …
  – Thus limited in usefulness and deployability
SNMPv3: Architecture

Application or Agent
- CG
- CR
- NG
- NR

Access Control
- VACM

Dispatcher

Message Processing
- SNMPv3 MP

Security
- User-based (USM)

SNMPv3 Engine

Network
- UDP
- TCP
- ...

Wes Hardaker <hardaker@sparta.com>
SNMPv3: Architecture

Application or Agent
- CG
- CR
- NG
- NR

Access Control
- VACM
-...

Dispatcher

Message Processing
- SNMPv3 MP
-...

Security
- User-based (USM)
- Integrated!
-...

Network
- UDP
- TCP
-...

SNMPv3 Engine

Modular & Extensible (Our new work)

Wes Hardaker <hardaker@sparta.com>

May 24, 2004
Goal: Integrated Security

• SNMPv3’s security component is extensible
  – It is easy to create a quick improvement
  – (This work will NOT be SNMPv4)

• Goal: add a new module with an integrated approach allowing you to use existing users.
  – Small & easy to implement addition == Fast
  – Ties to existing user authentication systems

• Requirements: YOUR INPUT
  – This work will not go forward unless YOU think it will helpful.
Quick Poll
(Here’s where you raise your hands)

- How many people use SNMPv3 today?
- How many people think it’s too hard to set up the user authentication?
- Would you use SNMPv3 if you could use your existing user account infrastructure?
Quick Poll

- What user authentication do you use today?
Identification Schemes
(which do you want?)

Used for:
• Local Accounts
• SSH Public-key Identities
• (Current SNMPv3/USM model)
Identification Schemes
(which do you want?)

Used for:
• Radius
• TACACS+
Identification Schemes
(which do you want?)

Used for:
• Kerberos
Identification Schemes (which do you want?)

Used for:
• PKI deployments (CA use is optional on both sides)
  (EG usage: TLS & SSL)
The Road Ahead

- Potential candidates already exist:
- **Session-Based Security Model (SBSM)**
  - Extensible authentication system
  - Even supports compression, many other +s
  - draft-hardaker-snmp-session-sm-01.txt
- **Kerberos based**
  - Implemented already in Net-SNMP >= 5.0
  - draft-hornstein-snmpv3-ksm-02
- **USM+** (Not yet published)
Questions & Answers

• Contact Information:
  Wes Hardaker <hardaker@sparta.com>
  David Perkins <dperkins@snmpinfo.com>

• Mailing List:
  – https://www.machshav.com/mailman/listinfo/sbsm

• Web Sites:
  – SBSM: http://sbsm.hardakers.net/
  – Electronic SURVEY on this site!
    • Please please please fill it out!