Internet Infrastructure Security Panel

Symposium on Network and Distributed System Security
February 10, 1997
Internet Infrastructure Security

• Panelists
  – Steve Bellovin - AT&T Research
  – Olafur Gudmundsson - TIS
  – Paul Lambert - Oracle
  – Russ Mundy - TIS
What Gives (or Doesn’t Give) the Internet Infrastructure Security?

• Interaction Between “Internet Pieces”

• Dominated By Protocols - Examples
  – Internet Protocol
  – Routing
  – Name Service
  – Network Management
  – etc, etc, etc,

• Software Implementing & Executing the Protocols
Internet Infrastructure Security Requires (at least)

- Support for Security Mechanisms in Protocols
  - Standards are Crucial
- Implementation and Use of Security Mechanisms in Software of “Internet Pieces”
- Policies and Correct Usage
Are All Internet Related Protocols Infrastructure? 
(one view)

- Infrastructure
  - OSPF, BGP, (add your favorite routing protocol(s))
  - DNS
  - ARP
  - SNMP
  - IP
  - ISAKMP/Oakley
  - DHCP

- Probably Not??
  - TCP
  - HTTP
  - FTP
  - Telnet
  - ....
Are All Internet Related Protocols Infrastructure? (another view)

- Everything Needed for MY Job
  An Example:
  - Email is Infrastructure to end users
  - TCP is Infrastructure to Email Developers
  - IP is Infrastructure to Multicast Developers and Users
Internet Infrastructure Security
How Much Is There??

• Some Today BUT More is Coming
• Emerging Protocol Standards
• Experimental & Reference Software Implementations
  Examples
  – IPSEC / ISAKMP / OAKLEY
  – DNSSEC
  – SNMP-NG
SNMP - Next Generation

Symposium on Network and Distributed System Security
February 10, 1997
SNMP ADVISORY TEAM

Background

- Chartered After 36th IETF
- Security and Administrative Framework Evolution for SNMP Advisory Team (AKA Advisory Team)
- Principal Goal: Identify Single Approach for SNMP-NG That Can Move to Open Working Group
SNMP ADVISORY TEAM

Approach Highlights

• Used As Much From Existing Technology Base as Practical
• Constrained to Requirements of Existing v2* & USEC Proposals
• Did Not Choose One “Winner”
• Identified a Set of Modules and Interfaces that Perform Required Functions
SNMP ADVISORY TEAM

Approach Highlights (cont)

• Approach Emphasizes Modularity
• Documents Expected to Follow the Modularity
• It Is Not Necessarily Expected that Implementations Will Choose To Follow Strict Modularity
• Currently Defined Security Services (Integrity & Confidentiality) Are Sufficient
USER-BASED SNMP-NG MODULES & SUB-MODULES

User-Based Security Model Processing

Message Processing, & Control

Management Application

Proxy Handling Application

Local Processing

Instrumentation

TrapTable

> DestinationAdrs

QOS

Security Model

TrapGroup

PDU Processing

View Lookup

View AccessControl

UserTable

> snmpEngineID

> userName

authProtocol

privProtocol

acGroup

SecurityCookie

Proxy Handling

Determine Naming Scope

Timeliness

Timeliness

Priv

Priv Table

after Table

Auth

Auth Table
GENERATE REQUEST_MSG

Security Model Processing

Message Processing, & Control

Determine Naming Scope

GlobalData
- ScopedPDU
- securityCookie

Local Processing

Transport

Application
- DestinationAdrs
- SecurityModel
- MMS
- SecurityCookie
- ScopedPDU

UserTable
- snmpEngineID
- userName
- authProtocol
- privProtocol
- acGroup
- SecurityCookie

View Lookup

V AC

PDU Processing

Instrumentation

Trap Table
- DestinationAdrs
- QOS
- Security Model
- Trap Group

Trap Processing

Priv

Auth

Timeliness

auth Table

time Table

priv Table
SNMP ADVISORY TEAM
Process Recommendations

• Re-Charter “standard” Working Group
• Develop Revised Documents With “Cut & Paste” Approach
• Plan Face-to-Face Meeting (or 2) Prior to April IETF
• Have I-D(s) Prepared Prior to April IETF
THANK YOU
Backup Slides
SNMP ADVISORY TEAM

Members

• David Harrington
• Jeff Johnson
• David Levi
• John Linn
• Russ Mundy
• Shawn Routhier
• Glenn Waters
• Bert Wijnen
SNMP Advisory Team

Message Format Illustrations
SNMP-NG MESSAGE FORMAT

Global Data
- Version
- MsgID
- MMS
- SecurityModel
- QOS/RptFlag

Security Model Information
SECURITY MODEL SPECIFIC DATA

Naming Scope
- ContextID
- ContextName

PDU
Per RFC-1905
(Includes Operations and Varbinds)

ScopedPDU
SNMP-NG MESSAGE FORMAT
User-Based Security Framework

Global Data

Security Model Information

Naming Scope

PDU

SECURITY MODEL SPECIFIC DATA

-User-Based General Param (snmpEngineID, Boots, Time, UserName)

-AuthParam (KeyedMD5 Digest)

-PrivParam (DES)

User-Based Security Framework
Model Information
RECEIVE SNMP-NG noAuth/noPriv MESSAGE

Security Model Processing
- MMS
- QOS
- ptr to SecurityModelData
- ptr to message

Determine Naming Scope

ScopedPDU-MMS
- Group
- SecurityCookie
- ScopedPDU

Management Application

Proxy Handling Application

TrapTable
- >DestinationAddr
- QOS
- Security Model
- TrapGroup

Local Processing

Instrumentation

View Lookup

V PDU Processing

UserTable
- >snmpEngineID
- >userName
- authProtocol
- privProtocol
- acGroup
- SecurityCookie

Auth Table

Auth

Timeliness

time Table

Priv Table

Priv

Transport
GENERATE SNMP-NG noAuth/noPriv MESSAGE

Security Model Processing
Message

1. UserTable
   - snmpEngineID
   - userName
   - authProtocol
   - privProtocol
   - acGroup
   - SecurityCookie

2. Authentication
   - GlobalData
   - ScopedPDU
   - securityCookie

3. Message Processing, & Control
   - Determine Naming Scope

   Proxy Handling Application
   - TrapTable
     >DestinationAddr
     QOS
     Security Model
     TrapGroup

   Local Processing
   - View Lookup
     V AC
     PDU Processing

   Management Application
   - Trap

   Transport

   Global Processing
   Auth
   TimeTable
   Priv Table
   TimeTimeliness
   authTable
   timeTable
   privTable
RECEIVE SNMP-NG Auth/noPriv MESSAGE

Security Model Processing
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Message Processing, & Control
- MMS
- QOS
- ptr to SecurityModelData
- ptr to message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing

RECEIVE SNMP-NG Auth/noPriv MESSAGE
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message

Determine Naming Scope

Local Processing

Transport

Management Application

Proxy Handling Application

Instrumentation

Trap Processing

View Lookup

V AC PDU Processing
GENERATE SNMP-NG Auth/noPriv MESSAGE

1. UserTable
   - snmpEngineID
   - userName
   - authProtocol
   - privProtocol
   - acGroup
   - SecurityCookie

2. timTable
   - timeliness
   - boots
   - time

3. privTable
   - priv

4. authTable
   - auth
   - data

5. Security Model Processing
   - userName
   - ptr to authParams
   - ptr to whole message

6. Message Processing, & Control
   - GlobalData
   - ScopedPDU
   - securityCookie

7. Transport

Management Application
Proxy Handling Application
Local Processing
Instrumentation
View Lookup
VAC
PDU Processing
TrapTable
>DestinationAddrs
QOS
Security Model
TrapGroup
Trap Processing
RECEIVE SNMP-NG Auth/Priv MESSAGE

Security Model Processing
- snmpEngineID
- userName
- ptr to authParams
- ptr to whole message
- snmpEngineID
- Boots
- Time
- ErrorCode
OR
ScopedPDU-MMS
- Group
- SecurityCookie
- userName
- ScopedPDU
- ptr to authParams
- ptr to encrypted message

Message Processing, & Control
- MMS
- QOS
- ptr to SecurityModelData
- ptr to message

Determine Naming Scope

Local Processing

UserTable
> snmpEngineID
> userName
authProtocol
privProtocol
acGroup
SecurityCookie

View Lookup

Proxy Handling Application

Management Application

Transport

Instrumentation

Trap Processing

TrapTable
> DestinationAddrs
QOS
Security Model
TrapGroup

Tis ISOC SNDSS, FEB 10, 97 , # 27
GENERATE SNMP-NG Auth/Priv MESSAGE

1. UserTable
   - snmpEngineID
   - userName
   - authProtocol
   - privProtocol
   - acGroup
   - SecurityCookie

2. Encrypted-ScopedPDU
   - userName
   - ptr to privParams
   - ptr to ScopedPDU

3. Security Model Processing
   - snmpEngineID
   - userName
   - ptr to authParams
   - ptr to whole message

4. Time Table
   - Timeliness
   - Boots
   - Time

5. GlobalData
   - ScopedPDU
   - securityCookie

6. Auth Table
   - Auth
   - data

7. Message Processing, & Control
   - snmpEngineID
   - userName
   - ptr to authParams
   - ptr to whole message

8. Determine Naming Scope
   - GlobalData
   - ScopedPDU
   - securityCookie

9. Transport
   - Management Application
   - Proxy Handling Application

View Lookup

V AC

PDU Processing
RECEIVE RESPONSE _ MSG

Security Model Processing
- ErrorCode
- OR
- ScopedPDU-MMS
- Group
- SecurityCookie
- ScopedPDU
- ModelSpecific
- SecurityStuff

Message Processing, & Control
- MMS
- QOS
- ptr to SecurityModelData
- ptr to message
- QOS
- ScopedPDU-MMS
- SecurityModelData
- MMS
- SecurityCookie
- ScopedPDU

Application
- SecurityCookie

Transport

Local Processing

UserTable
- > snmpEngineID
- > userName
- authProtocol
- privProtocol
- acGroup
- SecurityCookie

View
- Lookup

Instrumentation

TrapTable
- > DestinationAddrs
- QOS
- Security Model
- TrapGroup

PDU
- AC
- Processing
GENERATE RESPONSE_MSG

Security Model Processing

Message Processing, & Control

Determine Naming Scope

GlobalData
ScopedPDU
- securityCookie

Message

Local Processing

- ScopedPDU

Instrumentation

View Lookup

V AC PDU Processing

Proxy Handling Application

Management Application

Transport

auth Table

UserTable

&nameEngineID

>userName

authProtocol

privProtocol

acGroup

SecurityCookie

Priv

Timeliness

time Table

Auth

auth Table
PROXY PROCESSING
Overview

Proxy Application

Dual Role
SNMP
Engine/Entity

Agent Role

Manager Role

Request

Response

Response From
Proxyed Request

Proxyed Request

1 2 3 4 5 6 7 8