

# Replacing TripWire with SNMPv3

Matthew G. Marsh

Chief Scientist of the NebraskaCERT

# Scope

- Quick Overview & History of SNMP
- Definitions & Terminology

SNMPv3 will be implicit in the rest of the sections

- RFC(s) that define v3
- Highlights - why use v3
  - Authentication
  - Privacy
  - Security Scope
- General Usage
- Net-SNMP
- PakDefConX MIB
- PakDefConX Source Code
- Usage Example
- Discussion

# History

- SNMP is defined by four features:
  - A data definition language
  - Management Information definition
  - A protocol definition
  - Security and Administration definition
- Standard 15 defines the protocol (SNMP)
- Standard 16 defines the structure of management information
- Standard 17 defines MIB-II
- All SNMP information and organization is specified using Abstract Syntax Notation One (ASN.1) (ISO Standard)
- SNMPv1 came into being and use in the late 1980's. By 1990 most equipment capable of speaking TCP/IP used SNMPv1 for management capabilities. Some vendors, most notably WellFleet, used SNMP as the basis for all interaction with the equipment.
- SNMPv1 was defined by three modes of operation
  - Read - a mode of obtaining information from a device based on a query/response
  - Write - a mode of setting parameters within a device based on query/response
  - Trap - a mode for a device to send information about itself without a query
- These first two modes used basic single passwords as the authentication and security measures
- SNMPv1 was designed for and used UDP as the main transport mode
- Contrary to popular belief v1 did provide a framework for authentication, privacy, and authorization; however there were no actual protocol structures, designs, or implementations done within this framework.
- SNMPv2 came in several incarnations as it was developed. One of the primary original design goals for v2 was to structure and design authentication, privacy, and authorization. However this was not realized although much of the structure formality was completed.
- SNMPv2 added better data types and efficiency along with the first use of TCP for data transport confirmation
- SNMPv2 essentially came in three major flavours: v2c, v2u, v2\*(v2p)
  - V2c was "officially endorsed" but v2u/v2p had security structures (authentication, privacy, authorization)

# Definitions and Terminology

- Abstract Syntax Notation One (ASN.1) (ISO Standard)
  - 1.3.6.1 = .iso.org.dod.internet
  - This is the tree from whence all MIB things come... ;-}
- OID - Object ID is the reference to the ASN.1 code which defines an object
  - 1.3.6.1.4.1.9248 is the OID assigned to Paktronix Systems LLC
  - Paktronix Systems MIBs would begin from this OID and branch outward and downward
  - 1.3.6.1.4.1.9248.1.1.1 is the settable string of the file to be hashed and is fully decoded as:
    - .iso.org.dod.internet.private.enterprises.Paktronix.PakDC.PakSETFiles.PakTestFileString
- Structure of Management Information - SMI defines the structure of the data (data definition language)
  - SMIv1 is the format used in SNMPv1/v2
  - SMIv2 is the new extended improved format
- Community - the password used in v1 and v2c
  - Read was by popular default = public
  - Write was by popular default = private
- Agent - the device about which information is desired
  - Hub, router, coffee machine ^H^H Java Dispenser...
- Manager - the device which "manages" an agent
  - NetView, OpenView, Tivoli, Unicenter, etal are Managers
  - Managers typically query many remote agents but in some cases you can have a device that is both manager and agent in one.
- MIB - Management Information Base
  - Think of a database tree with all of the relevant information for a particular device
  - Generic MIB is called MIB-II (as opposed to MIB-I...) and is defined in RFC 1213
- Authentication - proving you are who you say you are (password/community/...)
- Privacy - encryption of the data in transport
- Authorization - Access Control applied to MIBs
  - Authorization is typically done by specifying subsets or even individual OIDs
- Trap - an Agent initiated data transfer

# RFC Documents

SNMP Version 3 is the current version of the Simple Network Management Protocol. This version was ratified as a Draft Standard in March of 1999.

-  RFC 2570: Introduction to Version 3 of the Internet-standard Network Management Framework, Informational, April 1999
-  RFC 2571: An Architecture for Describing SNMP Management Frameworks, Draft Standard, April 1999
-  RFC 2572: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), Draft Standard, April 1999
-  RFC 2573: SNMP Applications, Draft Standard, April 1999
-  RFC 2574: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), Draft Standard, April 1999
-  RFC 2575: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), Draft Standard, April 1999
-  RFC 2576: Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, Proposed Standard, March 2000

These documents reuse definitions from the following SNMPv2 specifications:

-  RFC 1905: Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), Draft Standard
-  RFC 1906: Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), Draft Standard
-  RFC 1907: Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), Draft Standard

## SNMP Version 3 - Important Points

- Authentication
  - MD5 or SHA authentication passphrase hashes
  - Passphrase must be greater than 8 characters including spaces
- Privacy
  - Packet data may now be DES encrypted (future use allows additional encryptions)
  - Passphrase defaults to authentication passphrase
  - Allows for unique Privacy passphrase
- Inform Traps
  - Old style trap was "throw-n-pray" over UDP
  - v2 Inform trap is over TCP and requires a response
  - Traps may also have Authentication and Privacy passphrases
- Security Structures
  - User / Scope / ACL all may have independent AuthPriv structures

## SNMP Version 3 - Authentication

- User
  - Defines the unit of access
- Group
  - Defines class for application of scope
- View
  - Defines a set of resources within a MIB structure
- Operation
  - Defines the actions that may be performed
    - READ
    - WRITE
    - ADMINISTER
- Operations are applied to Views
- Users are assigned to Groups
- Groups are assigned Views

## SNMP Version 3 - Privacy

- SNMP v1 and v2c transported data in clear text
- v3 allows the data payload to be encrypted
- Currently the specification only allows for DES
  - May be overridden for custom applications
  - Specification allows for multiple encryption mechanisms to be defined
- Passphrase defaults to using the authentication passphrase
  - Passphrase may be completely separate and unique
- Privacy must be specified in conjunction with authentication
  - Allowed: NONE, authnoPriv, authPriv

## SNMP Version 3 - Security Structures

- Passphrases are applied to User object only in current specification
  - Thus divorcing the ACL applied to the User from the AuthPriv functions
  - Each User object may have unique passphrases
- Specification extensions are being considered to allow
  - Passphrases for Groups
  - Passphrases for Views
  - Multiple Passphrases per User
    - Per Operation Mode
- Typically there is one User defined per Operation Mode

## SNMP Version 3 - Misc

- Implementation is requestor/provider model
- On Provider
  - Services through daemon process
  - Concept of "Engine ID"
    - Core of authPriv passphrases security
    - First pass hash mechanisms for storage
- On Requestor
  - Services through query of Provider
  - "Engine ID" also important
- Engine ID provides significant security addition through first pass hash

# General Usage Notes

- Use multiple Users
  - One for each action (get, set, trap)
  - Different Authentication passphrases
- Always use Privacy - authPriv
  - Make sure the passphrases are different from the User's
- For custom applications consider defining and using your own authentication and privacy encryption methods
  - PakSecured extensions use mhash libraries thus allowing use of any of the mechanisms they contain (see sourcecode)
  - Easily extensible to use mcrypt (or libraries of choice)
- Always set up your initial security in a secure environment before exposing the system to the elements.
- **SUMMARY: SNMP is a Message Passing Protocol.**

# Net-SNMP

- Net-SNMP has had v3 since 1998
- <http://www.netsnmp.org>
- \_the\_ reference application for SNMP
- Originally based on the Carnegie Mellon University and University of California at Davis SNMP implementations.
- Includes various tools relating to SNMP including:
  - An extensible agent
  - An SNMP library
  - Tools to request or set information from SNMP agents
  - Tools to generate and handle SNMP traps
- Can use multiple transports
  - IPv4 UDP/TCP
  - IPv6 UDP/TCP
  - IPX on Linux !!!

# PakDefConX MIB

 PakDefConX ::= { enterprises 9248 }  
 PakDC OBJECT IDENTIFIER ::= { PakDefConX 1 } -- The OBJECT IDENTIFIER for all PakDefConX tricks  
 PakSETFiles OBJECT IDENTIFIER ::= { PakDC 1 }

 PakTestFileString OBJECT-TYPE

SYNTAX OCTET STRING (SIZE(0..1024))

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"A publicly settable string that can be set for testing snmpsets. This value will eventually be used as the file name for the PakHash function.

::= { PakSETFiles 1 }

 PakTestFileHash OBJECT-TYPE

SYNTAX String

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"This object returns the md5sum of the file name set into PakFileTestString.

Only the md5sum is returned."

::= { PakSETFiles 2 }

# PakDefConX Source Code

- Source is provided as a patch against Net-SNMP v5.x
  - Tested on all versions up to 5.0.2.pre1 as of 7/8/2002
- Get Net-SNMP version 5 - CVS usually works best.
- Apply the patch (`patch -p1 < {patch file location}`)
- Edit the PakConfigure file in the source root dir
- Run the PakConfigure file (`bash PakConfigure`)
- `make; make install`
- Play
  
- Requires that mhash library 0.8.10 or greater be installed.
  - <http://mhash.sourceforge.net>

# The Point (why you are here...)

Assuming that you have the Net-SNMP patched and compiled:

Install an SNMPv3 user for the daemon

```
cat > /var/net-snmp/snmpd.conf
```

```
createUser defconx MD5 defconxv3 DES defconxcrypt ^D
```

```
cat > /usr/local/share/snmp/snmpd.conf
```

```
rwuser defconx ^D
```

Fire up the daemon - /usr/local/sbin/snmpd

Now to play with the mib defs:

```
snmpwalk -u defconx -l authPriv -a MD5 -A defconxv3 -x DES -X defconxcrypt localhost .1.3.6.1.4.1.9248
```

```
PAKDEFCONX-MIB::PakTestFileString.0 = STRING: "/etc/hosts"
```

```
PAKDEFCONX-MIB::PakTestFileHash.0 = STRING: "5b41d38e2a46d028902e3cecf808c582"
```

```
DEFINE {insert Stuff} = '-u defconx -l authPriv -a MD5 -A defconxv3 -x DES -X defconxcrypt'
```

```
snmpset {insert Stuff} localhost .1.3.6.1.4.1.9248.1.1.1.0 s "/etc/services"
```

```
PAKDEFCONX-MIB::PakTestFileString.0 = STRING: "/etc/services"
```

```
snmpwalk {insert Stuff} localhost .1.3.6.1.4.1.9248
```

```
PAKDEFCONX-MIB::PakTestFileString.0 = STRING: "/etc/services"
```

```
PAKDEFCONX-MIB::PakTestFileHash.0 = STRING: "24fd8b34bc51d3ebfab4784ca63a70e7"
```

FV Oiler.

# Comments, Critiques, CIA

---

- These are words that begin with a 'c'

# Replacing TripWire with SNMPv3

Matthew G. Marsh

Chief Scientist of the NebraskaCERT