(In)Security in Network Management

Security in distributed and remote network management protocols

Jeremy Rauch <jrauch@cadre.org>

Network Management

- ♦ What is it?
- ♦ Why do we need it?
- ◆What are our options with regard to selecting a network management scheme?
- ◆ What are the security flaws it can introduce
- ◆ What can be done to minimize the risk of these security flaws?

Network Management: What is it?

- **♦** Hardware
 - ◆ Switches, routers, firewalls, WAP's, hosts, printers
 - ◆ Just about anything on the network
- **♦** Software
- **♦** Protocols
- ◆ Allows for remote management of the network from convenient, centralized sites

Network Management: Why is it needed?

- ◆Lowers costs by eliminating the need for many administrators at multiple locations performing the same function
- ◆ Makes network administration and monitoring easier and more convenient
- Coherent presentation of data

Major NM Options

- ◆ SNMPv1
- ◆ SNMPv2c
- ◆ SNMPv3
- Vendor proprietary solutions
- ◆ Quite a few options that never panned out...
 - ◆ DCE
 - ◆ REAL SNMPv2
 - ◆ CMIP

SNMP Flaws...

- **♦** The Protocols
 - ◆ SNMPv1
 - ◆ SNMPv2
 - ◆ SNMPv2c
 - ◆ SNMPv3
 - ◆ RMON/RMON2

- **◆** The Implementations
 - ◆ Default communities
 - ◆ Buffer overflows
 - ◆ Design + Logic errors
 - Miscellaneous
- ◆ Applying it
 - Info gathering and network mapping
 - ◆ Network manipulation
 - ◆ Top secret new stuff

SNMPv1 History

- ◆Why was it created?
- ◆RFC 1157, 1990: "A Simple Network Management Protocol (SNMP)"
 - ◆RFC 1067, 1988
- ◆RFC 1155, 1158, 1990: Original specification of the MIBII

SNMPv1 Overview

- ◆ Information to be stored laid out in the Management Information Base (MIB)
- Specification of fields to be collected, data types, formatting, access controls
- ♦ Written in ASN.1
 - ◆ Easy to read
 - ◆ Not so fun to write
 - ◆ Basically akin to a Db schema
- ◆ Data encoded using BER

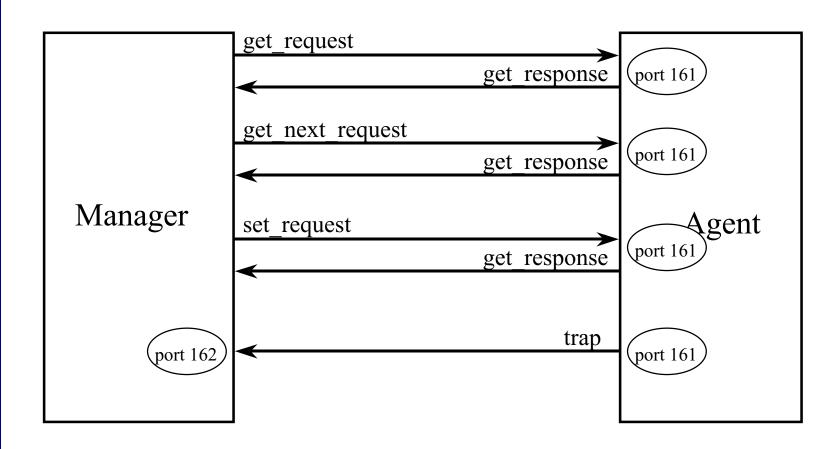
SNMP sample output

```
[1:38pm manager] snmpwalk agent public system
system.sysDescr.0 = Sun SNMP Agent, SPARCstation-20
system.sysObjectID.0 = OID: enterprises.42.2.1.1
system.sysUpTime.0 = Timeticks: (619954285) 71 days, 18:05:42.85
system.sysContact.0 = manager@cadre.org
system.sysName.0 = agent
system.sysLocation.0 = Under my desk
system.sysServices.0 = 72
[1:39 manager ] snmpwalk agent public
   ip.ipNetToMeduaTable.ipNetToMediaEntry.ipNetToMediaType
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.10.1.98.1 = other(1)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.1.10.1.98.2 = dynamic(3)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.2.10.1.98.36 = dynamic(3)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.2.10.1.98.37 = other(1)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.10.1.97.1 = other(1)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.10.1.97.101 = other(1)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.3.10.1.97.254 =
   dynamic(3)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.4.10.1.98.41 = dynamic(3)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.4.10.1.98.45 = other(1)
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType.7.10.1.96.1 = other(1
```

SNMPv1 Protocol

- ◆Five Simple Messages:
- ◆ get-request
- ◆ get-next-request
- ◆ get-response
- ◆ set-request
- **♦**trap

SNMPv1 Protocol continued...



SNMPv1 Protocol continued...

- **◆**UDP Transport Mechanism
- ◆ Community: Shared "password" between agent and manager
- ◆PDU: Specifies request type
- ◆Request ID
- **♦**Error Status
- **♦**Error Index

SNMPv1 Packet Format

UDP Header	Version	Community	PDU Type	Request ID	Error Status	Error Index	name	value	name		
---------------	---------	-----------	-------------	---------------	-----------------	----------------	------	-------	------	--	--

SNMPv1 Security Flaws

- **◆**Transport Mechanism
 - ◆ Data manipulation
 - ◆ Denial of Service
 - **♦** Replay
- Authentication
 - ♦ Host Based
 - Community Based
- **◆**Information Disclosure

SNMPv1 Transport Mechanism Flaws

- **♦**UDP Based
- ◆Unreliable packets may or may not be received
- ◆Easily forged trivial to forge source of packets

SNMPv1Authentication Flaws

- **♦**Host Based
 - ◆ Fails due to UDP transport
 - ◆DNS cache poisoning
- Community Based
 - Cleartext community
 - Community name prediction/brute forcing
 - ◆ Default communities

SNMPv1 Information Disclosure

- Routing tables
- ◆ Network topology
- ◆ Network traffic patterns
- ♦ Filter rules
- ◆ Vendor proprietary information + invocation
 - ◆ Execute arbitrary programs, etc

SNMPv1Security Flaw Implications

- ◆ Altering/Manipulation of network by unauthorized individuals
- ◆ Denial of Service on whole networks
- ◆ Modification of ACL's & configurations
- Clear topology of network behind router
- ◆ Makes creation of more sophisticated host based attacks easier

SNMPv2 History

- ◆RFC 1441, 1993: "Introduction to version 2 of the Internet-standard Network Management Framework"
- ◆RFC 1446, 1993: "Security Protocols for version 2 of the Simple Network Management Protocol"
- ◆ Written to address security and feature deficiencies in SNMPv1

SNMPv2 Protocol

- ◆Extension to SNMPv1
- ◆Provided security model
- ♦2 new commands
 - ◆ get-bulk-request
 - ◆ inform-request
 - ◆ Acknowledged trap
- ◆A big, big failure

SNMPv2 Security Flaws

- **♦** Replay
 - ◆ Clock synch required, but not specified
- Encryption attacks
 - ◆ DES known plaintexts, IV issues, etc
- Authentication attacks
 - ◆ MD5, user defined, no folding or expansion
- ◆ Transport + backwards compatibility

SNMPv2 Downfall

- ◆Marginal security
- Complex implementation
- ◆Devices were a whole lot slower and lacking in ram + horsepower

SNMPv2C

- ◆What is it?
- ♦ Why does it exist

SNMPv2C Protocol

- ◆SNMPv2 additional PDU types
- ◆SNMPv1 Community based authentication
- **◆**UDP transport
- ◆ All the features of SNMPv2 with the security of SNMPv1

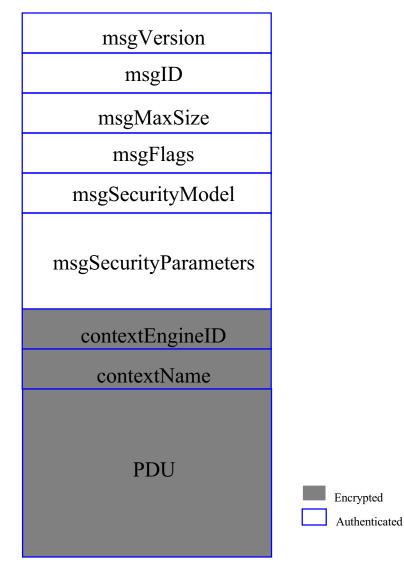
SNMPv3 History

- RFC 3410, 2002: "Introduction and Applicability Statements for Internet Standard Management Framework "
- ◆ RFC 3411, 2002: "An Architecture for Describing SNMP Management Frameworks"
- RFC 3412, 2002: "Message Processing and Dispatching"
- ◆ RFC 3413, 2002: "SNMP Applications"
- RFC 3414, 2002: "User-based Security Model"
- RFC 3415, 2002: "View-based Access Control Model"
- RFC 3416, 2002: "Version 2 of SNMP Protocol Operations"
- RFC 3417, 2002: "Transport Mappings"
- ◆ RFC 3418, 2002: "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)"
- ◆ RFC 2576, 2578, 2579, 2580...
- ◆ Written to address the failures of the original SNMPv2 security model

Protocol

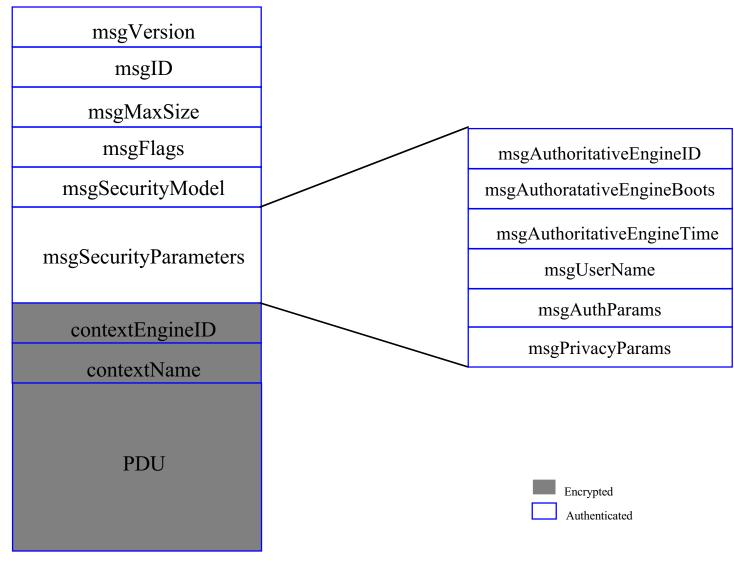
- Designed to be implementable and secure
 - ◆ Based on the original SNMPv2 work (SNMPv2u and SNMPv2*)
- ◆ Uses SNMPv2 PDU format + types
 - ◆ No new PDU types specified
- ◆ UDP transport
- ◆ Strong (enough) encryption and authentication
- ◆ New User-based Security Model
- New View-based Access Control (enhanced MIB view concept)
- ◆ Starting to catch on (kinda sorta)

Packet Format



Reference: "SNMP,SNMPv2, SNMPv3 and RMON 1 and 2, 3rd Edition", William Stallings, 1998

Packet Format: User-Based Security Model



Reference: "SNMP,SNMPv2, SNMPv3 and RMON 1 and 2, 3rd Edition", William Stallings, 1998

SNMPv3 User-based Control Model

- **◆**Encryption
 - **◆**DES
 - ◆ CBC mode
- **♦** Authentication
 - **♦**HMAC
 - ◆SHA-1
 - ♦ MD5
- **◆**Timeliness mechanism

SNMPv3 Flaws

- **◆** Encryption
 - ◆ CBC mode depends on 64 bit IV
 - ◆ IV is created by taking last 8 octets of 16 octet privKey (pre-IV)
 - ◆ 8 octet salt value is xored with the pre-IV to create the IV
 - ◆ Only the salt value is transmitted, in msgPrivacyParameters field
 - ◆ Problem: Salt generation is left as an exercise to the implementor
 - Brute force of bad passwords
 - Slowed by password to key mechanism

SNMPv3 Flaws

- **♦** Authentication
 - ◆ Handled via HMAC-{SHA-1, MD5}
 - ◆ Output truncated to 12 octets
 - **♦** MD5
 - ◆ 16 octet auth key
 - ◆ SHA-1
 - ◆ 20 octet auth key
 - ◆ Stored in msgAuthParameters
 - ◆ Actually, HMAC is an excellent authentication mechanism
 - ◆ Short auth password can be brute forced
 - ◆ Password to key mechanism slows down attack
 - ◆ Harder due to collisions due to truncated output

SNMPv3 Flaws

- **♦** Timeliness mechanism
 - ◆ Uses boot count + time since last reboot of agent
 - ◆ Transmitted via a 2-step synch mechanism + stored
 - ◆ snmpEngineBoots
 - ◆ snmpEngineTime
 - ◆ latestReceivedEngineTime
 - Can prevent replay attacks within window
 - ◆ 150 second skew allowed
 - ◆ Skew depends on authoritative v. non-authoritative recipient

SNMPv3 Realized...

- Pretty cool protocol
- ◆ Still susceptible to denial of service
 - ◆ But what isn't?
- ◆ Forgery possible, but difficult to abuse
- ◆ Brute forcing possible, but tough + slow
- ◆ Time based attacks may be possible
 - ◆ Immediate replay of packets MAY allow action invocation attacks
- ◆ Traffic analysis

RMON and RMON2 Security

- ◆SNMP's flaws
- additional hazards by introducing "action invocation" objects
- collects extensive info on subnet
- packet captures

Implementation Vulns

- **◆**Defaults
- ◆MIB designs
- ◆Buffer Overflows + parsing
- ◆Design + logic errors
- **♦**Miscellaneous

Default Communities

- public
- private
- write
- "all private" (sun)
- monitor (3com)
- manager (3com)
- security (3com)
- OrigEquipMfr (brocade)
- "Secret C0de" (brocade)
- secret
- cable-docsis
- xyzzy, agent_steal, freekevin, and fubar (?!)

- admin
- ◆ default
- password
- ILMI
- tivoli
- openview
- community
- ◆ snmp
- snmpd
- system (aix, others)
- ♦ And so on...

Hidden Communities

- ◆ An obscene percentage of managed devices contain hidden communities
- Often fully read/write privileged

MIB Designs

- ◆Too much info!
 - ◆ D-Link password disclosure
 - enterprises.937.2.1.2.2.0
 - ◆ Similar problems affect all "toy" routers
 - ◆Cisco VACM community disclosure
 - snmpVacmMIB.vacmMIBObjects.vacmAccessTable
 - ◆ A quick perusal of interesting keywords at www.mibdepot.com reveals hundreds of potential vulns

Buffer Overflows + Parsing

- ◆ OULU PROTOS evaluation
 - ◆ Identified hundreds of test cases for evaluating SNMP protocol implementations
 - ◆ Invalid BER length fields
 - Long strings
 - ◆ Format strings
 - ◆ Found dozens of implementation flaws
 - Most implementations derived from CMU/UCD/Net-SNMP
- Real world examples abound
 - ◆ IRIX snmpd overflow

Misc

- ◆ All sorts of "conveniences"
 - ◆ Cisco CONFIG-COPY.mib & CISCO-FLASH.mib
 - ◆http://www.cisco.com/warp/public/477/SNMP/copy configs s nmp.shtml
- Management stations not without own problems
 - ◆ Tivoli Netview execute arbitrary commands with a well formed trap under custom configs
- ◆ net-snmp has had client tool + agent flaws
 - ◆ Most recent one patched within the last few months

Applied SNMP Flaws (Demo)

- ◆ Network discovery and mapping
 - ◆ snmp host identification + network mapping

Applied SNMP Flaws (Demo)

- ◆ Network manipulation
 - ◆ ARP cache manipulation
 - ◆ Session teardown
 - ◆ Route manipulation

Applied SNMP Flaws (Demo)

◆Top Secret Stuff

Securing existing implementations

- ◆ Risk assessment
- Minimization of use
- ◆Allow get-*'s only, no remote setting
- ◆Eliminate defaults
- ◆Filtering EVERYWHERE
 - ◆ Marginally useful at best
- ◆ Management network

Sources you need to check out...

- Multiple SNMP RFC's (mentioned throughout talk)
- ◆ SNMP, SNMPv2, SNMPv3 and RMON 1 and 2, William Stallings (ISBN 0-201-4834-6)
- ◆ *TCP/IP Illustrated Volume 1*, Richard Stevens (ISBN
- www.mibdepot.com
- Simple Times (<u>www.simple-times.org</u>)
- OULU PROTOS (http://www.ee.oulu.fi/research/ouspg/protos/index.html)
- www.securityfocus.com
 - Vulnerability DB
 - Bugtraq
- ◆ Net-snmp (<u>www.net-snmp.org</u>)

Questions?