

# Internet infrastructure

Prof. dr. ir. André Mariën

# SNMP

# SNMP

- Simple Network Management Protocol
  - RFC 1157
- An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
  - STD: 62
- Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
  - RFC 3416

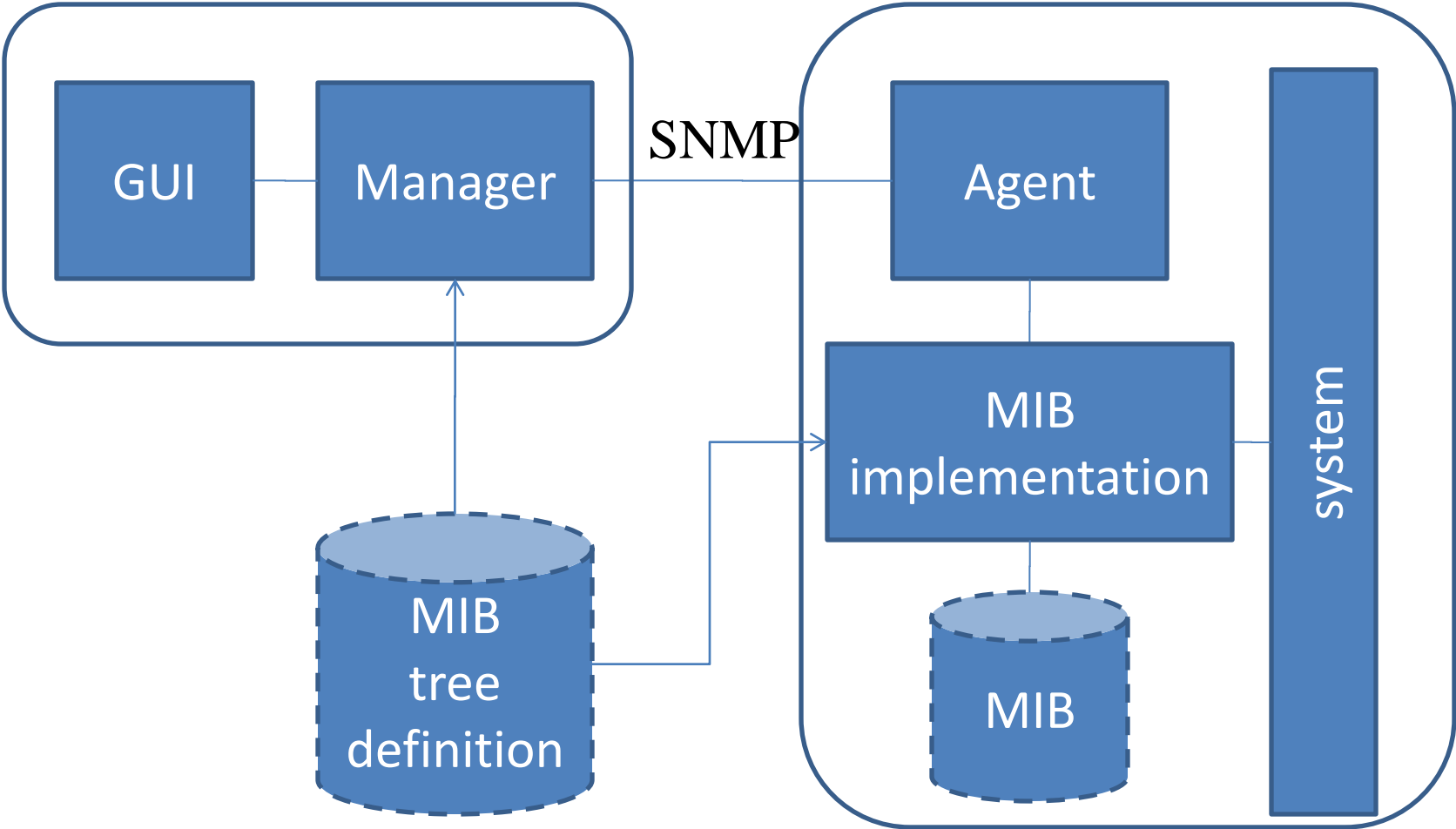
# Version 3

- RFC 3411. An Architecture for Describing SNMP Management Frameworks (December 2002)
- RFC 3412. Message Processing and Dispatching (December 2002)
- RFC 3414. User-based Security Model (December 2002)
- RFC 3415. View-based Access Control Model (December 2002)
- RFC 3418. Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (December 2002)
- RFC 3826. The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model

# Components of a SNMP management system

- Managed nodes
  - each with an SNMP entity containing command responder and notification originator applications
  - access to management instrumentation (agents)
- On or more SNMP entities containing command generator and/or notification receiver applications (“manager”)
- a management protocol

# High level view



# Management Information Base (MIB)

- Defines a tree
- Tree consists of objects
- Objects have identifiers
- Defines set/get methods on these elements
  - Compare with Java Bean properties

# Creating a MIB

- Abstract Syntax Notation One (ASN.1)
- Used to describe MIB
- Vendor subtree

# Example from RFC

-- request/response information

RequestID ::= INTEGER

ErrorStatus ::= INTEGER { noError(0), tooBig(1),  
noSuchName(2), badValue(3), readOnly(4) genErr(5)  
}

ErrorIndex ::= INTEGER

-- variable bindings

VarBind ::= SEQUENCE { name ObjectName, value  
ObjectSyntax }

VarBindList ::= SEQUENCE OF VarBind

# Object identifier: tree walking

- iso org dod internet mgmt mib system  
sysDescr => 1 3 6 1 2 1 1 1

# Agents

- On the managed system, there is an agent
- It receives requests and sends answers
- “set/get” may result in (significant) code execution before producing the answer
- For convenience: also: getnext (enumeration)
- Authentication of requests: community string (combination of userID and password)

# Basic SNMP messages

- GET
  - Retrieve value for an element of the MIB
  - Uses OID tyo identify value
- GETNEXT
  - Tree walking: request values depth-first
- SET
  - Modify value of MIB element
- TRAP
  - Agent sends unsolicited respons
- INFORM/RESPONS (v2)

# Management stations

- Server side: management stations
- Simple GUI/complex systems with autodiscovery etc.
- HP openview, SUN Solstice, IBM Tivoli (Netview), ...
  
- Simple solutions: SNMP tree browsers

# Security objectives

- Primary, SHOULD provide protection:
  - Modification of Information
  - Masquerade
- Secondary, SHOULD provide protection are:
  - Message Stream Modification
    - The SNMP protocol is typically based upon a connectionless transport service which may operate over any subnetwork service.
    - The re-ordering, delay or replay of messages may happen in normal operation
    - Messages may be maliciously re-ordered, delayed or replayed to an extent which is greater than normal
    - May lead to unauthorized management operations
  - Disclosure
    - threat of eavesdropping

# Remote Configuration

- The Security and Access Control Subsystems add a whole new set of SNMP configuration parameters
- The Security Subsystem also requires frequent changes of secrets at the various SNMP entities.
- To make this deployable in a large operational environment, these SNMP parameters must be remotely configurable.

# Goals of the SNMP Security Model

- Detect Modification:
  - SNMP message not modified in transit
- Ensure Authentication:
  - Source authentication
- Ensure timeliness:
  - detection of messages that are not recent
- Confidentiality:
  - protect from disclosure

# Constraints

1. When the requirements of effective management in times of network stress are inconsistent with those of security, the design of (User Security Model) USM has given preference to the former.
2. Neither the security protocol nor its underlying security mechanisms should depend upon the ready availability of other network services (e.g., Network Time Protocol (NTP) or key management protocols).
3. A security mechanism should entail no changes to the basic SNMP network management philosophy.

# Measures

- Authentication
  - Message authentication
  - HMAC-MD5-96 authentication protocol
    - HMAC: Keyed-Hashing for Message Authentication: RFC 2104
- Encryption
  - CBC-DES Symmetric Protocol

# View-based Access Control Model

Access is a function of

- who: securityModel, securityName
- how: securityModel, securityLevel
- why: read, write, notification
- where: contextEngineID (constant), contextName
- what: objectName
- which: objectInstance

# Example MIB-2: RFC 1213

- Data organized in subsets
  - System - Interfaces - IP - ICMP - TCP - UDP - EGP - Transmission – SNMP
- System
  - sysDescr , sysObjectID , sysUpTime , sysName , sysServices
- interfaces
  - ifNumber, ifTable , ifEntry , ifDescr
  - ifType (ethernet-csmacd, fddi, ds1, ppp, ...)
  - ifMtu , ifInOctets , ifInErrors
- IP
  - ipForwarding , ipDefaultTTL , ipForwDatagrams , ipFragOKs , ipFragCreates , ipRouteTable , ipRouteEntry
- Icmp
  - icmpInMsgs , icmpInErrors , icmpInTimeExcds