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 3412. Message Processing and Dispatching (December 2002)
- RFC 3415. View-based Access Control Model (December 2002)
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
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
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
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 to identify value

• **GETNEXT**
  – Tree walking: request values depth-first

• **SET**
  – Modify value of MIB element

• **TRAP**
  – Agent sends unsolicited response

• **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
SNMPv3: security

- SNMPv3 adds security to SNMP
- Security is intended to be orthogonal to future core SNMP version changes
- It provides authentication, integrity and confidentiality
- It protects against replay via timechecking
- It uses shared secrets
- Secret management is outside of the specification
- It uses the notion of authoritative service (depends on the use case if it is the sender or the receiver)
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
Authentication and integrity

- Secret key signing is used for authentication and integrity
- Both parties share a secret
- The secret is configured/exchanged outside of the protocol
- The check uses
  - Message content
  - Time
  - Sender & receiver
  - Secret
- Measures
  - Message authentication
  - HMAC-MD5-96 authentication protocol
    - HMAC: Keyed-Hashing for Message Authentication: RFC 2104
Timeliness

• The messages contain a timestamp
• Messages with reasonable times are accepted
• The non-authoritative side of the communication synchronizes its time notion with the authoritative side
• As an extra measure, number of boots is used
Confidentiality

• Here too a shared key is used
• The encryption uses DES, or CBC with DES
  – Enhanced to use AES
• The IV for CBC is derived from SNMP parameters