Verteiltes Internet Management

Jürgen Schönwälder

Institut für Betriebssysteme und Rechnerverbund
TU Braunschweig
Bültenweg 74/75
38106 Braunschweig

E-Mail: schoenw@ibr.cs.tu-bs.de
Tel.: 0531 / 391-3289

Übersicht

- Einführung in das Internet Management
- Structure of Mangement Information Version 2 (SMIv2)
- Simple Network Management Protocol Version 3 (SNMPv3)
- Sicherheit und Zugriffskontrolle in SNMPv3
- Management by Delegation (MbD) im Internet
- JASMIN Prototyp (TU Braunschweig / NEC C&C Research Berlin)
- Diskussion

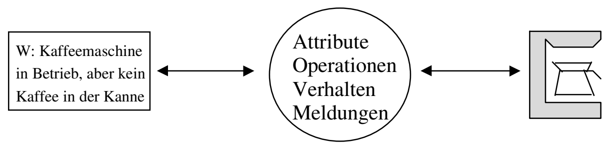
Motivation

- Aktuelle Situation:
  - Wachsende Bedeutung der strategischen Ressource "Information".
  - Ein Rechnernetz ist nicht mehr nur ein unterstützendes Element in einem Unternehmen, sondern nimmt immer häufiger eine Schlüsselstellung ein.
  - Die Anzahl der vernetzten Rechner ist in den letzten Jahren sprunghaft gestiegen. Dieser Prozeß wird vermutlich weiter andauern.
  - Die Komplexität und Funktionalität der Komponenten wächst enstprechend der Leistungssteigerungen der zugrundeliegenden Hardware.
- Forderung:
  - Ständige Verfügbarkeit der Netzdienste mit bestmöglicher Qualität.
  - Reduktion der Kosten für den Betrieb der Netzinfrastruktur.
- Notwendigkeit:
  - Rechnergestütztes Management heterogener Netze.

Begriff des „Managed Object“ (MO)

- Die Kontrolle, Koordination und Überwachung von Betriebsmitteln erfolgt durch die Manipulation von sogenannten Managed Objects:

  "A managed object is the abstracted view of a resource that presents its properties as seen by (and for the purpose of) management." (ISO 7498-4)
- Managed Objects sind also eine abstrakte Repräsentation einer realen Ressource.
- Die Grenze (boundary) eines Managed Objects bestimmt, welche Details einem Management-System zugänglich sind.



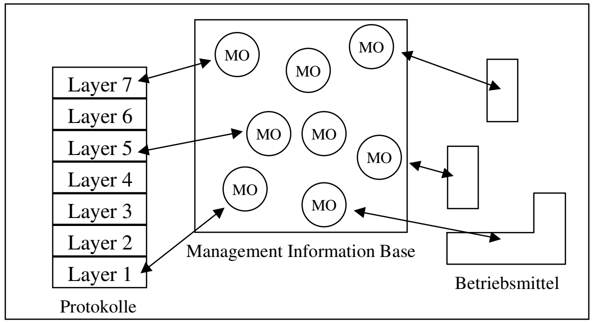
Management-System Managed Object Reales Betriebsmittel

➤ Die Managed Objects entsprechen nicht unbedingt Objekten, wie man sie aus der objekt-orientierten Programmierung kennt. (Insbesondere im Internet-Management entsprechen den MOs einfache Variablen.)

Management Information Base (MIB)

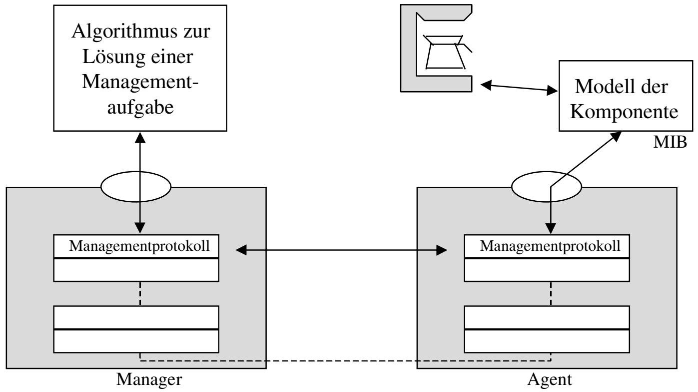
- Die Menge aller Managed Objects eines Systems bildet die Management Information Base (MIB) des Systems:

  "The set of managed objects within a system, together with their attributes, constitutes that system's management information base." (ISO 7498-4)
- Diese ISO/OSI Terminologie findet auch im Internet Anwendung.

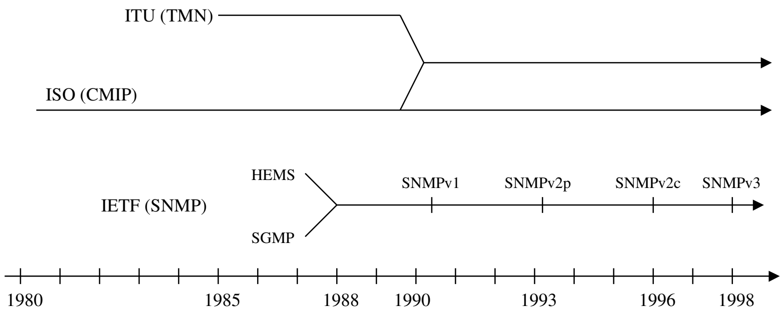


Managementprotokoll

- Managementanwendung und Managed Objects befinden normalerweise nicht auf demselben System.
- Ein Managementprotokoll realisiert den Zugriff auf entfernte Managed Objects.



Entwicklung der SNMP Technologie



- SNMP Version 1 (SNMPv1) war sehr erfolgreich und ist die derzeit installierte Basis.
- Party-based SNMP Version 2 (SNMPv2p) war zu komplex, um eingesetzt zu werden.
- Community-based SNMP Version 2 (SNMPv2c) ist eine Variante von SNMPv2 ohne Sicherheit, die langsam an Verbreitung gewinnt.
- SNMP Version 3 (SNMPv3) ist eine sichere Erweiterung von SNMPv2 mit breiter Unterstützung durch die Hersteller. Der Erfolg am Markt bleibt abzuwarten.

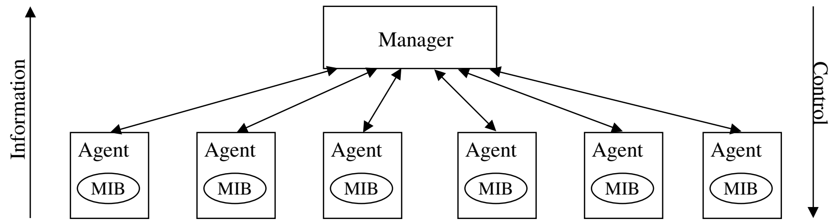
Ziele beim Entwurf von SNMP

- Minimierung der Anzahl und der Komplexität der Managementfunktionen, die durch einen Agenten realisiert werden:
  - ➥ Reduktion der Entwicklungskosten für Management-Agenten
  - ➥ Gleiche Managementtechnologie für alle Geräte, egal ob Drucker oder Cray
  - ➥ Entwicklung von neuen Managementfunktionen ohne die Agenten ständig verändern zu müssen.
- Erweiterbarkeit durch neue MIB-Definitionen.
- Unabhängigkeit von existierenden Rechner- oder Netzwerkarchitekturen.
- Robustheit durch einen einfachen, verbindungslosen Transportdienst.
- Keine Abhängigkeit von anderen Netzdiensten.

➤ Einige dieser ursprünglichen Ziele haben mittlerweile an Bedeutung verloren.

➤ Das "simple" bezieht sich auf die Anforderungen, die zur Laufzeit an ein Gerät gestellt werden und nicht auf die Spezifikationen oder den Implementations-aufwand für Managementapplikationen.

Trap-Directed Polling



- SNMP-Manager pollt in regelmäßigen Intervallen die SNMP-Agenten.
- Agenten können einem Manager durch sogenannte Traps Ausnahmesituationen signalisieren.
- Der SNMP-Manager kann die Pollingstrategie beim Empfang von Traps anpassen (trap-directed polling).

➤ Streng zentralisiertes Modell, in dem der Manager die ganze Funktionalität und Verantwortung trägt.

Übersicht

✓ Einführung in das Internet Management

✐ Structure of Mangement Information Version 2 (SMIv2)

Simple Network Management Protocol Version 3 (SNMPv3)

Sicherheit und Zugriffskontrolle in SNMPv3

Management by Delegation (MbD) im Internet

JASMIN Prototyp (TU Braunschweig / NEC C&C Research Berlin)

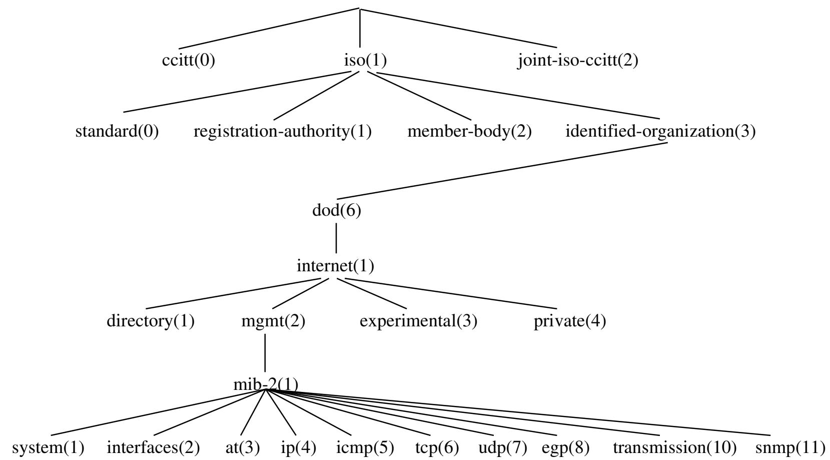
Diskussion

Informationsmodell (SMIv2)

- Das Management-Informationsmodell wird als "Structure of Management Information" (SMI) bezeichnet und beruht auf typisierten Variablen (Objekttypen).
- Jede Variable ist von einem einfachen (nicht zusammengesetzten) ASN.1 Datentyp:
  - `INTEGER, OCTET STRING, OBJECT IDENTIFIER, NULL`
  - `Integer32, Unsigned32, Counter32, Counter64, Gauge32`
  - `IpAddress, TimeTicks, BITS, Opaque`
- Variablen treten entweder einzeln auf (Skalare) oder sie bilden eine Spalte in einer konzeptionellen Tabelle.
- Auf den Variablen können lediglich die Operationen "lesen" und "schreiben" angewendet werden. Das SNMP-Protokoll erlaubt jedoch die Manipulation von Listen von Variablen.
- SMIv2 Management Information Bases (MIBs) werden mit Hilfe von ASN.1-Makros definiert, wobei die SMIv2 die ASN.1 Regeln angepaßt/erweitert hat.

Registration und Struktur der MIB-II

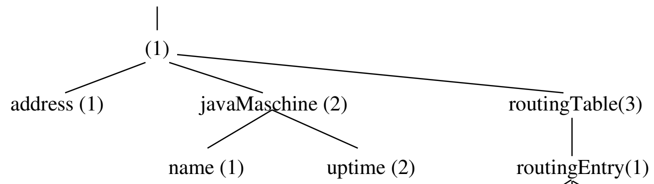
- Alle Objekttypen werden im ISO/OSI Registrationsbaum registriert.

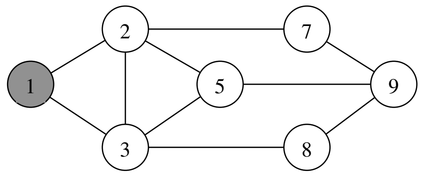


Object Identifier und Instance Identifier

- Durch die Registration kann jeder Objekttyp eindeutig mit einem Object Identifier identifiziert werden.
- Konkrete Ausprägungen eines Objekttyps werden durch einen sogenannten Instance Identifier eindeutig benannt.
- Durch das Anhängen des Instance Identifiers an den Object Identifier ergibt sich eine eindeutige Bezeichung einer Instanz eines Objekttyps.
- Skalare haben grundsätzlich nur eine Instanz, wobei der Instance Identifier grundsätzlich den Wert 0 hat.
- Instance Identifier für nicht-skalare Variablen werden aus dem eindeutigen Schlüssel der konzeptionellen Tabelle abgeleitet.
- Durch die Längenbegrenzung von Object Identifier Werten in SNMP (max. 128 Sub-Identifier) können Instance Identifier nicht beliebig komplex werden.

Einfache Beispiel-MIB mit einer Routing-Tabelle





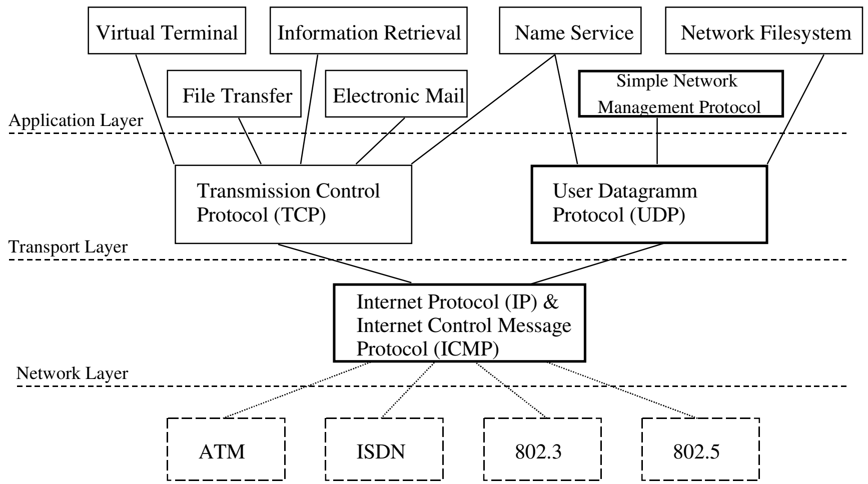
index(1)	dest(2)	next(3)
1	2	2
2	3	3
3	5	2
4	7	2
5	8	3
6	9	3

➤ Zur Vereinfachung werden im Beispiel Adressen durch natürliche Zahlen dargestellt.

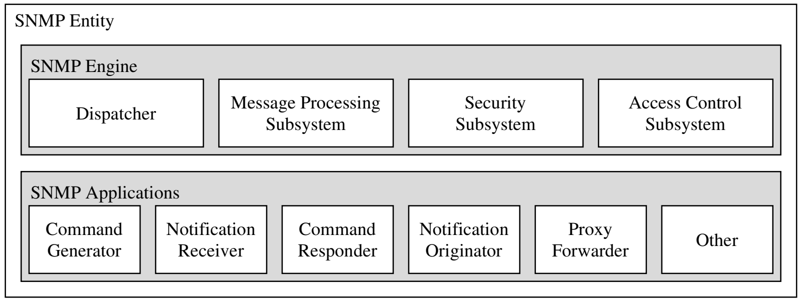
Übersicht

- ✓ Einführung in das Internet Management
- ✓ Structure of Mangement Information Version 2 (SMIv2)
- ✎ Simple Network Management Protocol Version 3 (SNMPv3)
- Sicherheit und Zugriffskontrolle in SNMPv3
- Management by Delegation (MbD) im Internet
- JASMIN Prototyp (TU Braunschweig / NEC C&C Research Berlin)
- Diskussion

Internet - Protokollübersicht

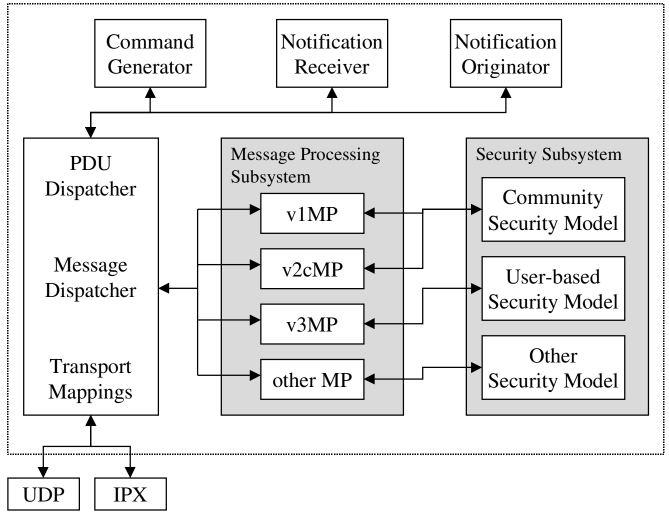


Architekturmodell von SNMPv3 (RFC 2271)

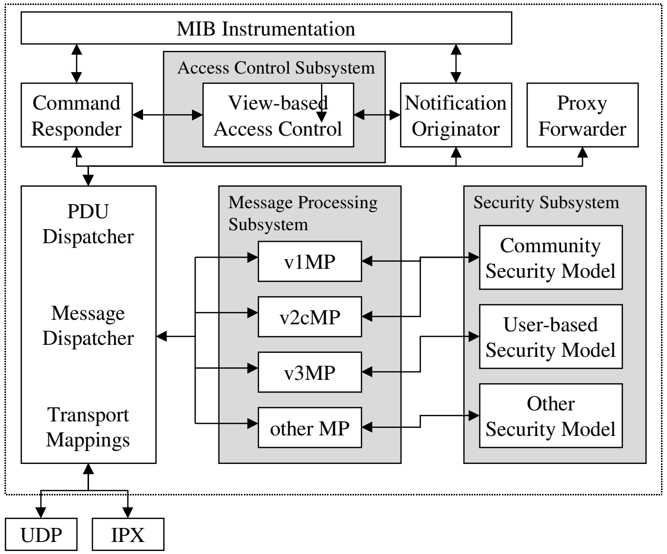


- Die SNMP-Engine eines SNMP-Entity besteht aus mehreren Subsystemen und einem Dispatcher.
- Für jedes Subsystem kann es mehrere Realisierungen geben.
- Das Manager/Agenten-Modell wird durch eine Reihe kleinerer „Applikationen“ ersetzt.
- Die Modularisierung erlaubt eine inkrementelle Weiterentwicklung von SNMP.

SNMP-Manager im SNMPv3 Architekturmodell



SNMPv3-Agent im SNMPv3 Architekturmodell



SNMPv3 Nachrichtenformat (RFC 2272)

SNMPv3Message:

msgVersion	msgGlobalData	msgSecurityParameter	msgData (scopedPDU)

MsgGlobalData:

msgID	msgMaxSize	msgFlags	msgSecurityModel

UsmSecurityParameter:

msgEngineID	msgEngineBoots	msgEngineTime	msgUserName	msgAuthParams	msgPrivParams

ScopedPDU:

contextEngineID	contextName	SNMPv2 PDU (as defined in RFC 1905)

- Security-Informationen befinden sich in der Mitte der Nachricht.
- msgData enthält entweder eine ScopedPDU oder eine verschlüsselte ScopedPDU.
- Die msgID wird zur Zuordnung von Antworten zu ausstehenden Anfragen benutzt.
- Die msgSecurityParameter sind abhängig vom msgSecurityModel.

Lexikographische Ordnung

- Gegeben sind zwei Folgen von natürlichen Zahlen $(x_1, x_2, ..., x_n)$ und $(y_1, y_2, ..., y_m)$ und es sei n <= m. Es gilt

  $$(x_1, x_2, ..., x_n) < (y_1, y_2, ..., y_m)$$

  genau dann, wenn einer der beiden folgenden Bedingungen erfüllt ist:

  (a) $x_j = y_j \quad 1 <= j < k$
  $x_k < y_k \quad k <= n$ und $k <= m$

  (b) $x_j = y_j \quad 1 <= j <= n$ und $n < m$

- Alle MIB-Instanzen können durch die Registration des Objekttyps und den Instance Identifier gemäß der lexikographischen Ordnung angeordnet werden.

- SNMP-Protokolloperationen arbeiten nur auf der lexikographischen Ordnung und nicht etwa auf konzeptionellen Tabellen oder der Baumstruktur der Registration.

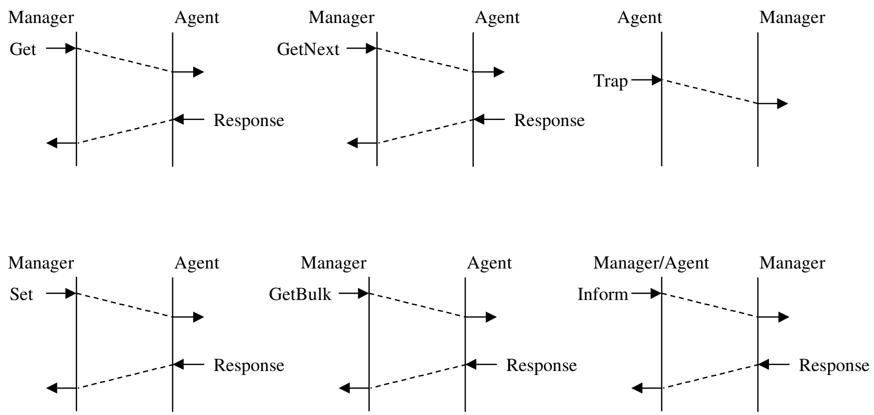
Beispiel zur lexikographischen Ordnung

- Betrachtet wird die Beispiel-MIB mit der einfachen Routing-Tabelle:

Object Identifier:	Wert:	Object Identifier	Wert:
1.1.0	10.1.2.3	1.3.1.2.4	7
1.2.1.0	"FilterFresh"	1.3.1.2.5	8
1.2.2.0	54321	1.3.1.2.6	9
1.3.1.1.1	1	1.3.1.3.1	2
1.3.1.1.2	2	1.3.1.3.2	3
1.3.1.1.3	3	1.3.1.3.3	2
1.3.1.1.4	4	1.3.1.3.4	2
1.3.1.1.5	5	1.3.1.3.5	3
1.3.1.1.6	6	1.3.1.3.6	3
1.3.1.2.1	2		
1.3.1.2.2	3		
1.3.1.2.3	5		

- Durch diese Anordnung geht die konzeptionelle Tabellenstruktur verloren.
- Die Felder einer Tabelle erscheinen Spaltenweise und nicht etwa Zeilenweise in der lexikographischen Ordnung.

SNMPv2/SNMPv3 Protokoll-Operationen (RFC 1905)



SNMPv2/SNMPv3 PDU-Formate (RFC 1905)

GetRequest, GetNextRequest, SetRequest, Trap, InformRequest:

PDU type	request-id	0	0	variable-bindings

GetResponse:

PDU type	request-id	error-status	error-index	variable-bindings

GetBulkRequest:

PDU type	request-id	non-reps	max-reps	variable-bindings

variable-bindings:

$name_1$	$value_1$	$name_2$	$value_2$	...	$name_n$	$value_n$

Übersicht

- ✓ Einführung in das Internet Management
- ✓ Structure of Mangement Information Version 2 (SMIv2)
- ✓ Simple Network Management Protocol Version 3 (SNMPv3)
- ✎ Sicherheit und Zugriffskontrolle in SNMPv3
- Management by Delegation (MbD) im Internet
- JASMIN Prototyp (TU Braunschweig / NEC C&C Research Berlin)
- Diskussion

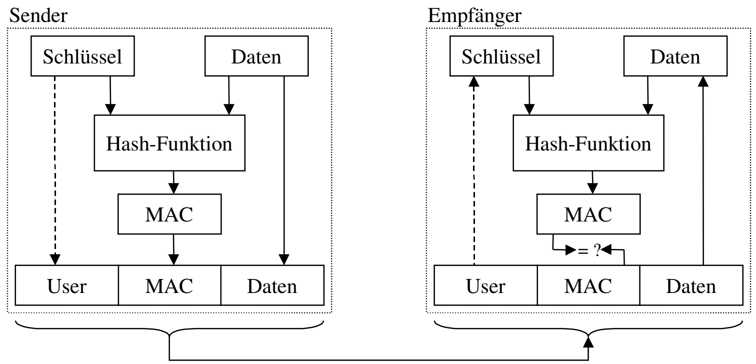
Sicherheitsproblematik

- Fragen, die bei der Entscheidung, ob eine Operation auszuführen ist, beantwortet werden müssen:
  - ① Ist die empfangene Nachricht authentisch?
  - ② Wer möchte die Operation ausgeführt bekommen?
  - ③ Welche Objekte sind von der Operation betroffen?
  - ④ Welche Rechte hat derjenige, der die Operation ausgeführt bekommen möchte, in Bezug auf die betroffenen Objekte?
- Die Fragen 1 und 2 werden durch die Maßnahmen zur Sicherung der Nachrichten beantwortet (Authentifikation, Verschlüsselung).
- Die Fragen 3 und 4 werden durch ein Modell zur Zugriffskontrolle beantwortet.

Authentifikation in SNMPv3 (RFC 2274)

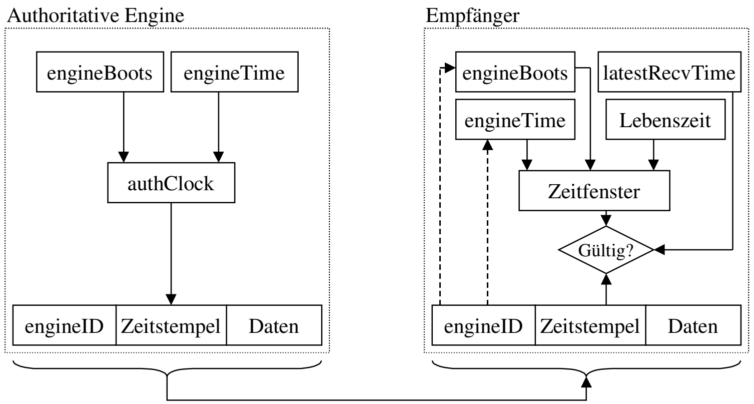
- Kryptographisch starke Hash-Funktionen (MD5, SHA-1) zur Bestimmung von kryptographisch starken Prüfsummen (Message Authentication Codes, MAC).
- HMAC (keyed hashing):
  - ➥ Bestimme zwei Schlüssel K1 und K2 von einem Schlüssel K.
  - ➥ Berechne T = Hash(K2 |M)
  - ➥ Berechne M´ = Hash(K1 | T)
  - ➥ Die ersten 96 bits von M´ sind der MAC der Nachricht M.
- ➥ Sicherung gegen Wiederholungen von alten Nachrichten durch lose synchronisierte Uhren und Zeitstempel.
- ➥ Algorithmische Erzeugung von Schlüsseln aus einem Passwort durch Anwendung einer Hash-Funktion auf eine 1 MB lange Konkatenation des Passworts.
- ➥ Ableitung „lokalisierter“ Schlüssel für die einzelnen SNMP Engines.

Datenintegrität und Authentifikation



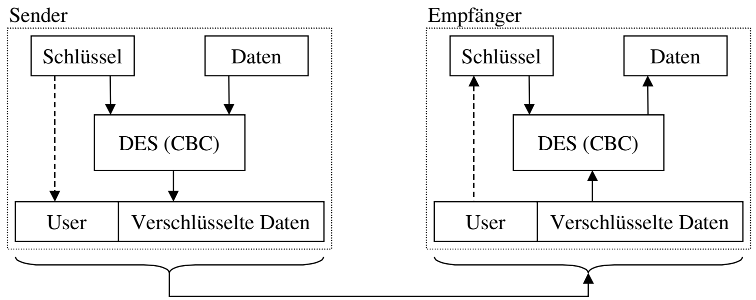
- Authentifizierung mit Message Authentication Codes (MAC) ist effizient zu realisieren.
- Die Hash-Funktion muß kryptographisch stark sein und einen „guten“ MAC erzeugen.
- Der MD5-Algorithmus (RFC 1321) läßt sich mit akzeptabler Performanz in Software realisieren (128 bit Digest).
- Der Secure Hash Algorithmus 1 (SHA-1) gilt derzeit als stärker im Vergleich zu MD5.

Sicherung gegen Wiederholungen von alten Nachrichten



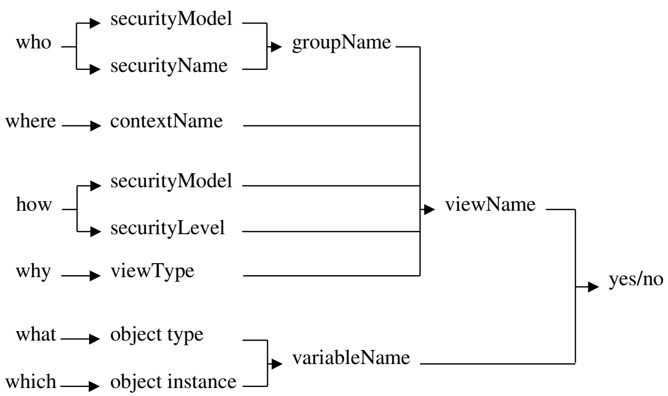
- Ein Empfänger muß die „Uhrzeit“ der für die Nachricht authoritiven SNMP-Engine kennen.
- Liegt die empfangene Nachricht im Gültigkeitsintervall und ist sie „jünger“ als die letzte gültige Nachricht, dann wird die Nachricht bearbeitet und es werden die Uhren angepaßt.
- Vor dem Beginn einer authentifizierten Kommunikation müssen die Uhren synchronisiert werden.

Sicherung gegen unbefugtes Abhören



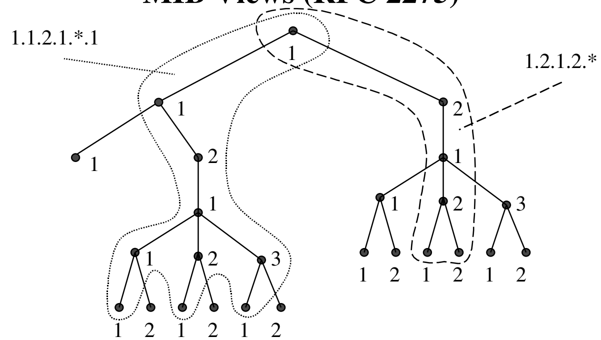
- Zur Sicherung gegen ein Abhören von Daten kann die ScopedPDU optional verschlüsselt werden.
- Zur Verschlüsselung wird der Data Encryption Standard (DES) in Cypher Block Chaining Modus (CBC) verwendet.
- Die Verschlüsselung ist relativ aufwendig und sollte nur in Situationen eingesetzt werden, in denen eine Verschlüsselung wirklich erforderlich ist.
- SNMPv3 erlaubt eine „relativ sichere“ Schlüsseländerung ohne Verschlüsselung.

Zugriffskontrolle in SNMPv3 (RFC 2275)



- Der securityLevel bestimmt, ob eine Nachricht ohne Authentifizierung (noAuth/noPriv), mit Authentifizierung (auth/noPriv) oder mit Authentifizierung und Verschlüsselung (auth/priv) versendet wird.
- Der securityName ist ein vom securityModel unabhängiger Name.

MIB Views (RFC 2275)



- Ein view subtree ist die Menge aller MIB-Objekte, die einen gemeinsamen OID-Präfix besitzen.
- Eine view tree family ist die Kombination von einem view subtree OID-Präfix mit einer Bitmaske, die bestimmt, ob ein Element des Präfixes signifikant ist oder nicht.
- Ein MIB-View setzt sich aus einer Menge von view tree families zusammen.
- Zugriffsrechte werden an einem read view, write view oder notify view definiert.

Eigenschaften und Probleme der Zugriffskontrolle

- Die Zugriffsentscheidung wird einzig und allein auf Grund der Information und Struktur des „Namens“ (Identifier des Objekttypen + Instance Identifier) getroffen.
- Durch eine geeignete Struktur der MIB lassen sich mit Hilfe von Bitmasken die Anzahl der benötigten Zugriffskontrollregeln in den Regelfällen reduzieren.
- Die Überprüfung von Zugriffsregeln in einem Agenten kann sehr teuer sein, da oftmals nicht bekannt ist, wieviele Instanzen bei einer GetNext oder GetBulk Operation „übersprungen“ werden müssen.
- Die Zugriffkontrolle in RFC 2275 erlaubt es nicht, einen securityName in mehreren Gruppen zu halten. Als Folge werden ähnliche, aber leicht unterschiedliche Zugriffsregeln für verschiedene securityNames sehr aufwendig zu konfigurieren.
  - ➥ Derzeit eine „heiße“ Diskussion zu diesem Thema in der SNMPv3 WG.

Übersicht

- ✓ Einführung in das Internet Management
- ✓ Structure of Mangement Information Version 2 (SMIv2)
- ✓ Simple Network Management Protocol Version 3 (SNMPv3)
- ✓ Sicherheit und Zugriffskontrolle in SNMPv3
- ✐ Management by Delegation (MbD) im Internet
- JASMIN Prototyp (TU Braunschweig / NEC C&C Research Berlin)
- Diskussion

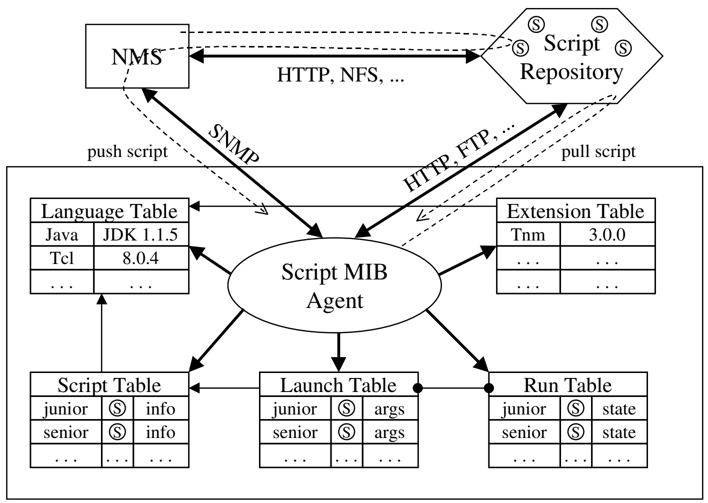
Probleme mit dem zentralisierten SNMP-Modell

- Zentralisierte Managementsysteme skalieren extrem schlecht:
  - ➥ Hohe Kommunikationskosten um die MIB-Daten zu den Applikationen zu befördern, die sie verarbeiten.
  - ➥ Parallel laufende Management-Applikationen benötigen eine extrem schnelle und damit sehr teure Hardware im zentralen Managementsystem.
- Überwachung von geographisch weit verteilten Netzwerken ist sehr kostenintensiv.
- Das zentrale Managementsystem ist ein „single point of failure“.
- Keine Unterstützung zur Delegation von Zuständigkeiten in großen Organisationen.

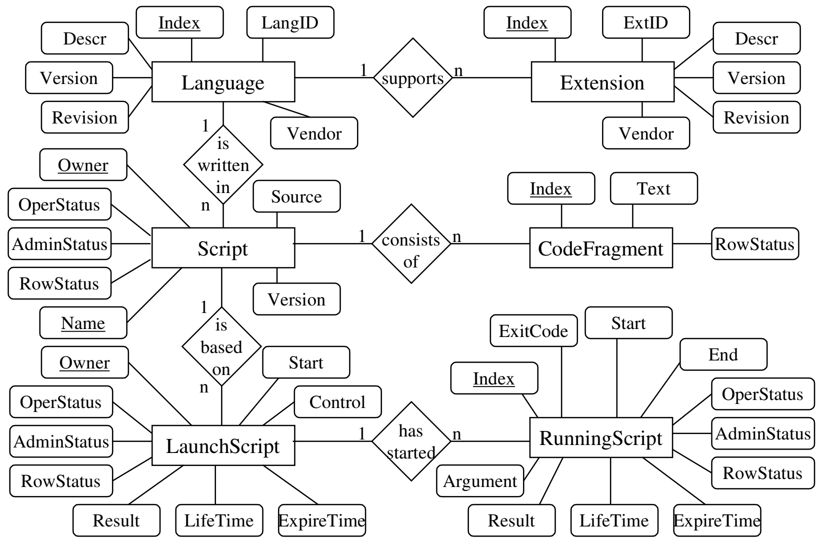
Management By Delegation

- Idee: Statt die Daten mit Hilfe von Management-Protokollen zu den Applikationen zu bringen, werden die Applikationen zu den Daten gebracht.
- Anstatt eine vordefinierte Funktion auf einem anderen System aufzurufen (Remote Procedure Call), wird der Programmtext der Funktion beim Aufruf mit übertragen (Remote Evaluation).
- Vorteile dieses Modells:
  - ➥ Reduktion des Netzwerkmanagement-Verkehrs
  - ➥ Größere Unempfindlichkeit gegenüber Netzwerkstörungen
  - ➥ Skalierbarkeit durch dezentrale Verarbeitung von Managementinformationen
  - ➥ Kostenersparnisse durch ein „offline-Management“
- Probleme liegen in der Wahl einer geeigneten Sprache und der Sicherheit des verwendeten Laufzeitsystems bzw. des Kommunikationsprotokolls.

Funktionsweise der IETF Script MIB



Vereinfachte Struktur der IETF Script-MIB



Sicherheitsaspekte der Script MIB

- Die MIB-Definition enthält Attribute, die die maximale Laufzeit von Skripten oder die Anzahl der parallelen Aufrufe eines Skripts begrenzen.
- Die Indizierung der MIB-Tabellen erfolgt über ein Owner-Attribut und geeignete „Hilfsknoten“ im Registrationsbaum, um das aktuelle SNMP Zugriffskontroll-modell halbwegs effizient anwenden zu können.
- Das Owner-Attribut kann in ein Betriebssystem security profile und ein security profile für das Laufzeitsystem abgebildet werden.
- Das Betriebssystem security profile beschreibt die Menge der Betriebssystem-Ressourcen, die ein laufendes Skript benutzen darf.
- Das security Profile des Laufzeitsystems kann Dienste der Laufzeitumgebung weiter einschränken (Java Sandboxen, Tcl padded cells).

Übersicht

✓ Einführung in das Internet Management

✓ Structure of Mangement Information Version 2 (SMIv2)

✓ Simple Network Management Protocol Version 3 (SNMPv3)

✓ Sicherheit und Zugriffskontrolle in SNMPv3

✓ Management by Delegation (MbD) im Internet

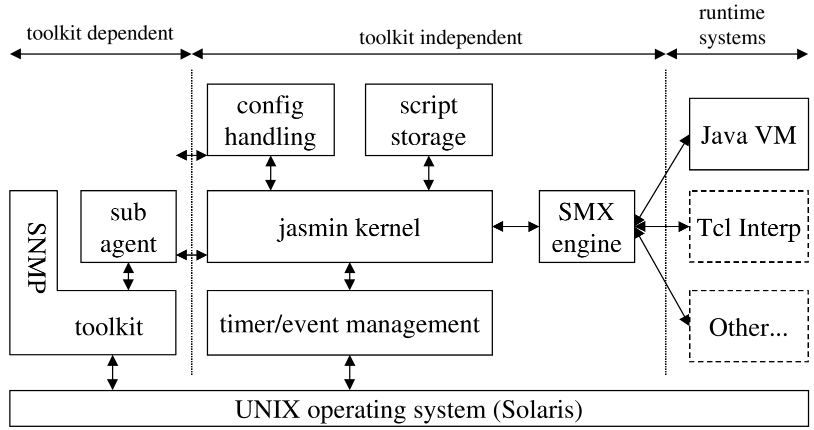
✐ JASMIN Prototyp (TU Braunschweig / NEC C&C Research Berlin)

Diskussion

Jasmin - Java Script MIB Implementation

- Ziele:
  - Bewertung der vorgeschlagenen Script MIB durch eine Implementation und den Test in konkreten Einsatzfällen.
  - Benutzung einer virtuellen Java Maschine als primäre Laufzeitumgebung.
  - Definition von „Schnittstellen“, mit denen neue Laufzeitumgebungen mit geringem Aufwand integriert werden können (plug in).
  - Rückmeldung von gewonnenen Erfahrungen in die Standardisierung.
- Kooperationspartner:
  - J. Quittek, A. Kind, J. Nicklisch, Cornelia Kappler (C&C Research Labs, NEC Europe Ltd., Berlin)
  - J. Schönwälder, M. Bolz, S. Mertens (Technische Universität Braunschweig)
- Weitere Informationen:
  - http://www.ibr.cs.tu-bs.de/projects/jasmin/

Interne Struktur von Jasmin



- Das SMX Protokoll trennt die Laufzeitumgebungen (die tatsächlich Skripte ausführen) von dem SNMP-Agenten, der die Script MIB implementiert.

Jasmin SNMP-Agent

- SNMP-Agent realisiert in „C“ unter Verwendung des Emanate SNMP-Toolkits.
- Keine Benutzung der vom MIB-Compiler generierten Datenstrukturen, um die Implementation leichter auf andere SNMP-Toolkits portieren zu können.
- Ungefähr 12.000 kommentierte Zeilen C/lex/yacc Quelltext für den Toolkit unabhängigen Teil der Implementation.
- Ungefähr 600 Zeilen modifizierter Quelltext, der ursprünglich vom MIB-Compiler generiert wurde.
- Benutzt GNU wget um Skripte via HTTP oder FTP von einem Repository zu laden. (Kleine Änderungen waren notwending, um Fehlercodes zugreifbar zu machen.)
- Ein „trusted binary“ wird benutzt, um eine sichere UNIX-Umgebung aufzusetzen. (Setzen der Unix uid/gid, Wechsel des root Verzeichnisses, Setzen von Limits)

Jasmin Java-Laufzeitumgebung

- Basiert auf JDK 1.1.5 und unterstützt alle JDK packages außer java.applet und java.awt.*.
- Mehrere Skripte können gleichzeitig in einer Laufzeitumgebung mit demselben runtime security profile ausgeführt werden.
- Die runtime system security profiles werden durch einen speziellen Java security manager und einen speziellen Java class loader realisiert.
- Java Skripte (Sammlungen von Java Klassen) müssen als jar Archive vorliegen.
- Implementiert in 99% purem Java. (Es war notwendig einen „C“ Funktion zu schreiben, um Zugriff auf die Environment-Variablen des UNIX-Prozesses zu erhalten.)
- 2.100 Zeilen kommentierter Java Quelltext für das komplette Java Laufzeitszstem. (800 Zeilen core engine, 600 Zeilen SMX Protokoll, 700 Zeilen runtime security)

Projektstatus

- Der Prototyp ist im Internet erreichbar, um ihn mit eigenen Skripten zu testen:
  - SNMP-Agent läuft auf osborne.ibr.cs.tu-bs.de, Portnummer 161.
  - SNMPv1/SNMPv2c community „junior“ oder „senior“.
  - SNMPv3 user „junior“ oder „senior“ (noAuth/noPriv, empty context).
- Derzeit bekannte Einschränkungen in Bezug auf die Script MIB Definition:
  - Das SNMP-Toolkit erlaubt es nicht wirklich, das abstrakte isAccessAllowed() Dienstprimitiv aufzurufen.
  - Die smCodeTable ist derzeit nicht implementiert.
- Geplante Aktivitäten:
  - Implementierung einer Tcl-Laufzeitumgebung (basierend auf SMX).
  - Implementierung von einigen Management-Skripten, um den Entwicklungs- und Testzyklus für Skripte besser zu verstehen.

Weitere Informationen

- JASMIN Web-Seite:

  http://www.ibr.cs.tu-bs.de/projects/jasmin/

- Script-MIB und SMX Spezifikation:

  D. Levi, J. Schönwälder: Definitions of Managed Objects for the Delegation of Management Scripts, <draft-ietf-disman-script-mib-06.txt>, November 1998

  J. Schönwälder, M. Bolz, M. Mertens, J. Quittek, A. Kind, J. Nicklisch: SMX - Script MIB Extensibility Protocol Version 1.0, Informatik-Bericht 98-07, Oktober 1998

- Weitere Dokumente:

  J. Schönwälder, J. Quittek: Secure Management By Delegation within the Internet Management Framework, Proc. 6th International Symposium on Integrated Network Management, Mai 1999

  J. Schönwälder: Network Management by Delegation - From Research Prototypes Towards Standards, Computer Networks and ISDN Systems 29(15), November 1997

Übersicht

- ✓ Einführung in das Internet Management
- ✓ Structure of Mangement Information Version 2 (SMIv2)
- ✓ Simple Network Management Protocol Version 3 (SNMPv3)
- ✓ Sicherheit und Zugriffskontrolle in SNMPv3
- ✓ Management by Delegation (MbD) im Internet
- ✓ JASMIN Prototyp (TU Braunschweig / NEC C&C Research Berlin)
- ✎ Diskussion