



••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

Netzwerksicherheit

Revisionsmechanismen

Stephen Wolthusen





Ziele von Revisionsmechanismen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Analyse und Verifikation der Wirksamkeit eingesetzter Sicherheitsmechanismen
- Erkennung von auffälligen Verhaltensmustern, Angriffen
- Möglichkeit zur forensischen Analyse von abgeschlossenen Vorfällen
- Unterstützung von straf- und zivilrechtlichen Verfolgungsmaßnahmen
- Sammlung und Verarbeitung von Revisionsdaten, insbesondere personenbezogener Daten, müssen gesetzlichen Bestimmungen entsprechen





BSD Syslog

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Eingeführt in 4.2BSD (September 1983)
 - Mechanismus wurde ad hoc entwickelt
 - Es existieren weder Unterlagen zu Design noch eine Spezifikation von `syslog(3C)`

- De facto Standard für Erzeugung und Verbreitung von Nachrichten
 - Erlaubt lokale Protokollierung
 - Protokollierung an beliebig vielen Hosts im Netzwerk ist ebenfalls möglich
 - Verfügbar auf (fast) allen Plattformen





Komponenten

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ syslog besteht aus zwei Komponenten

- Erzeugung von Nachrichten
 - ▲ Unter Unix meist direkt durch einen system call oder durch libc-Funktionen (`openlog(3C)`, `syslog(3C)`...)
 - ▲ Implementierung stark systemspezifisch, da kritisch für Geschwindigkeit (Solaris: STREAMS-Modul)
- Entgegennahme von Nachrichten
 - ▲ Lokal (Dateisystem/STREAMS)
 - ▲ Via Netzwerk (UDP Port 514), unter Unix: `syslogd`





Konfiguration (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Textdatei bestehend aus Blöcken von Zeilen, Block besteht aus
 - Selector unterteilt in
 - ▲ Facility
 - △ Quelle der Nachricht (`auth`, `authpriv`, `cdaemon`, `ftp`, `kern`, `...`, `security`, `user`, `...`, `local0`)
 - ▲ Level
 - △ Gibt Grad der Schwere der Meldung an (auch: Severity)
 - Aktionsanweisung





Konfiguration (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Zulässige Werte für Severity

- emerg: Kritisch für den Betrieb des Systems
- alert: Unmittelbare Behebung ist notwendig
- crit: Gravierende Fehler, z.B. nicht behebbare Gerätefehler
- err: Sonstige Fehler
- warning: Kein Fehler, aber trotzdem Handlungsbedarf
- info: Nur zur Information, kein direkter Handlungsbedarf
- debug: Zur Fehlersuche in aussendenden Programmen
- none: Nachricht sollte ignoriert werden





Konfiguration (3)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Gültige Aktionen:

- Datei: Meldung wird an Datei angehängt
- Hosts: Nachricht wird an syslog-Dienst auf Host weitergeleitet
- Nutzer-Konsolen: Meldung an lokal angemeldete (namentlich aufgeführte) Nutzer
- Alle Nutzer-Konsolen: Meldung an alle angemeldeten Nutzer
- Skripte: FreeBSD und OpenBSD erlauben die Ausführung beliebiger Skripte als Aktionsanweisung (Bourne-Shell)
 - ▲ Flexibel und mächtig
 - ▲ Große Gefahr der Ausnutzung durch DoS-Angriffe





Bestrebungen zur Standardisierung

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Dokumentation des Syslog-Protokolls durch IETF-Arbeitsgruppe „Security Issues in Network Event Logging“ seit Sommer 2000
 - Erste (!) Spezifikation in RFC 3164 (August 2001; neuer Entwurf vom 2. Dezember 2003)
 - Problem: Nur Codifizierung bestehender Systeme, Beobachtung von Verhaltensmustern/Analyse existierender Implementierungen
 - Einige weitere Ziele der Standardisierung
 - ▲ Zuverlässige Auslieferung
 - ▲ Authentisierte Übertragung
 - ▲ Sequenzierung von Meldungen





Nachrichtenformat von syslog

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Gesamtlänge muß unter 1024 Bytes liegen, drei Teile
- PRI
 - 3-5 Bytes, codieren Facility und Severity numerisch „<123>“
 - (Facility * 8) + Severity (Darstellung als Dezimalzahl)
- HEADER
 - Zeitstempel, codiert als „MMMddhh:mm:ss“
 - Quellangabe: IP-Adresse (v4 oder 6) oder Hostname
 - Jeweils getrennt durch Blank, nur druckbare Zeichen
- MSG
 - 7 Bit ASCII, keine Formatvorgabe





Erweiterungen für Syslog (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Authentizität

- Assoziation zwischen Absender einer Nachricht und Nachricht ist nicht gegeben
- Plausibilitätsprüfung nach Schnittstellen bei Relais-Architekturen nicht möglich, sonst nur rudimentär

■ Integrität

- Außer IP/UDP-Prüfsumme besitzt syslog keinen Schutzmechanismus

■ Vertraulichkeit

- syslog kennt nur Klartext-Nachrichten

■ Priorisierung





Erweiterungen für Syslog (2)

... department security technology ... department security technology ... department security technology ... department security technology ...

- Sequenzierung
 - Bei Übertragung über ein Netzwerk ist die Reihenfolge der Nachrichten nicht garantiert; Zeitstempel sind nicht ausreichend: Wichtig für forensische Analyse
- Schutz vor Wiedereinspielung
 - Da kein Integritätsschutz können Zeitstempel beliebig manipuliert werden
- Nachrichtenverlust
 - IP und UDP sind „best effort“-Protokolle
 - Nachrichten können unbemerkt verloren gehen/unterdrückt werden





Reliable Delivery

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ RFC 3195

- beschreibt Verwendung von TCP-Strömen zur Übertragung von syslog-Datensätzen
- Verwendet BEEP-Format zur Übertragung (XML-basiert)
- RAW-Modus
 - ▲ Verwendet Nachrichtenformat von syslog
- COOKED-Modus
 - ▲ Erweiterte Informationen und Struktur der Nachrichtenelemente





syslog-sign Entwurf (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Definiere drei Arten von Blocks
 - Reguläre Nachrichten
 - Signaturblöcke
 - Zertifikatsblöcke

- Reguläre Nachrichten bleiben gegenüber RFC 3164 unverändert

- Jeder Signaturblock enthält Signaturen über n Nachrichten
 - Enthält Hashes über n Nachrichten
 - Nicht alle Nachrichten sind zur Verifikation erforderlich
 - Datenformat entspricht regulären syslog-Nachrichten

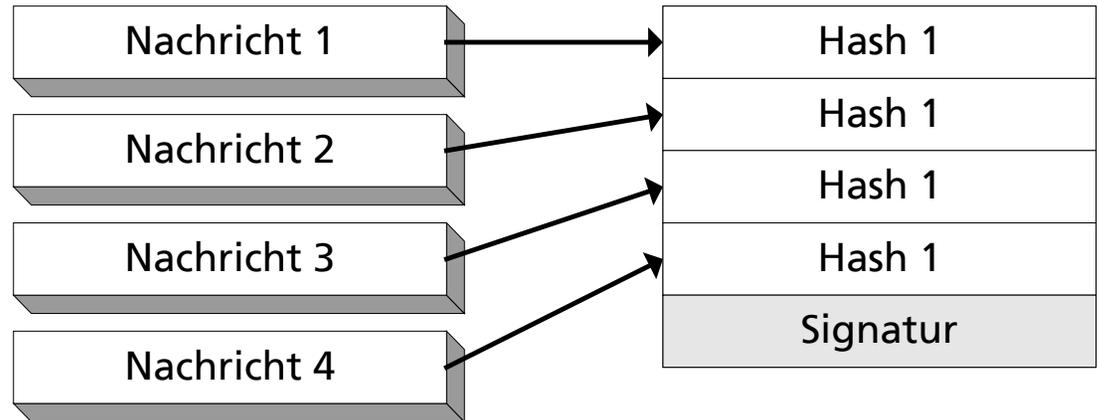




syslog-sign Entwurf (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Reihenfolge der Nachrichten muß nach Empfang anhand der Hash-Werte rekonstruiert werden
- Dies ist online nur ineffizient möglich





Inhalt der Signaturblöcke

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- PRI, HEADER entsprechen regulärer Nachricht; Base64-codierter Block wird mit Cookie „@#sigSIG“ eingeleitet
- Version: Protokollversion, Signaturschema
- Reboot Session ID: Darf sich während „Lebendauer“ der Nachrichtenquelle nicht wiederholen
- Global Block Counter: Gesamtzahl der von der Nachrichtenquelle versandten Nachrichten während Lebensdauer
- First Message Number: Erste Nachricht in diesem Hash-Block
- Count: Anzahl der Hash-Werte in diesem Block
- Hash Block: Sequenz der Hash-Werte
- Signature: Digitale Signatur gemäß ausgewähltem Schema





Inhalt der Zertifikatsblöcke

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Für Sitzungs- und Schlüsselverwaltung erforderliche Daten
 - werden genau einmal erzeugt
 - können größer als 1024 Bytes sein: Aufteilung in Blöcke

- Payload Block besteht aus:
 - Zeitstempel: Gibt Beginn der Reboot Session an
 - Signature Group Descriptor
 - Höchster SIG-Wert
 - Key Blob-Typ: PKIX-Zertifikat, Preshared, Signierter PK
 - Key Blob: Base64-codierte Rohdaten





Bewertung

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Viele syslogd-Implementierungen (Solaris!) lassen Nachrichten „fallen“ wenn ernsthafte Belastung vorliegt
- Keine Möglichkeit seitens eines Senders den Empfang zu prüfen oder eine Bestätigung zu erzwingen
- Dennoch wurden die Unzulänglichkeiten lange Zeit ignoriert
 - Auch kommerzielle Firewalls sind meist auf syslog beschränkt
- Umsetzung der syslog-Erweiterung dürfte noch mehrere Jahre dauern
 - Daher sind abwärtskompatiblen Nachrichtenformate extrem wichtig





Das Simple Network Management Protocol

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Die Verwaltung von TCP/IP-Netzwerken war lange Zeit eine Sammlung von ad hoc-Werkzeugen (ping, tcpdump, dig...)
- Wunsch nach systematischerer Vorgehensweise, partiell inspiriert durch die Mechanismen aus dem OSI-Bereich (ca. 1988).

Kandidaten:

- HEMS (High Level Entity Management System)
 - ▲ Verallgemeinerung eines Vorgängers, Host Monitoring Protocol
- SNMP (Simple Network Management Protocol)
 - ▲ Weiterentwicklung des SGMP von 1987
- CMOT (Common Management Information Protocol over TCP/IP)
 - ▲ Portierung des OSI-Management-Systems





Entwicklung von SNMP

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Zielsetzung des IAB: kurz/mittelfristige Entwicklung von SNMP („schnell und schmutzig“), langfristig Migration auf CMOT
 - Damals war man noch der Meinung, daß OSI TCP/IP mittelfristig ablösen würde
- Zur Erleichterung der Migration sollte SNMP bereits die für CMOT erforderlichen Datenbanken für verwaltete Objekte (Management Information Base, MIB) verwenden sowie Repräsentation dieser Datenbank
 - Unrealistisch, daher doch parallele Weiterentwicklung
- RMON für Fernüberwachung von MIBs





Management-Architektur von SNMP

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- SNMP basiert auf vier Grundelementen
 - Management Station
 - Management Agent
 - Management Information Base
 - Network Management Protocol

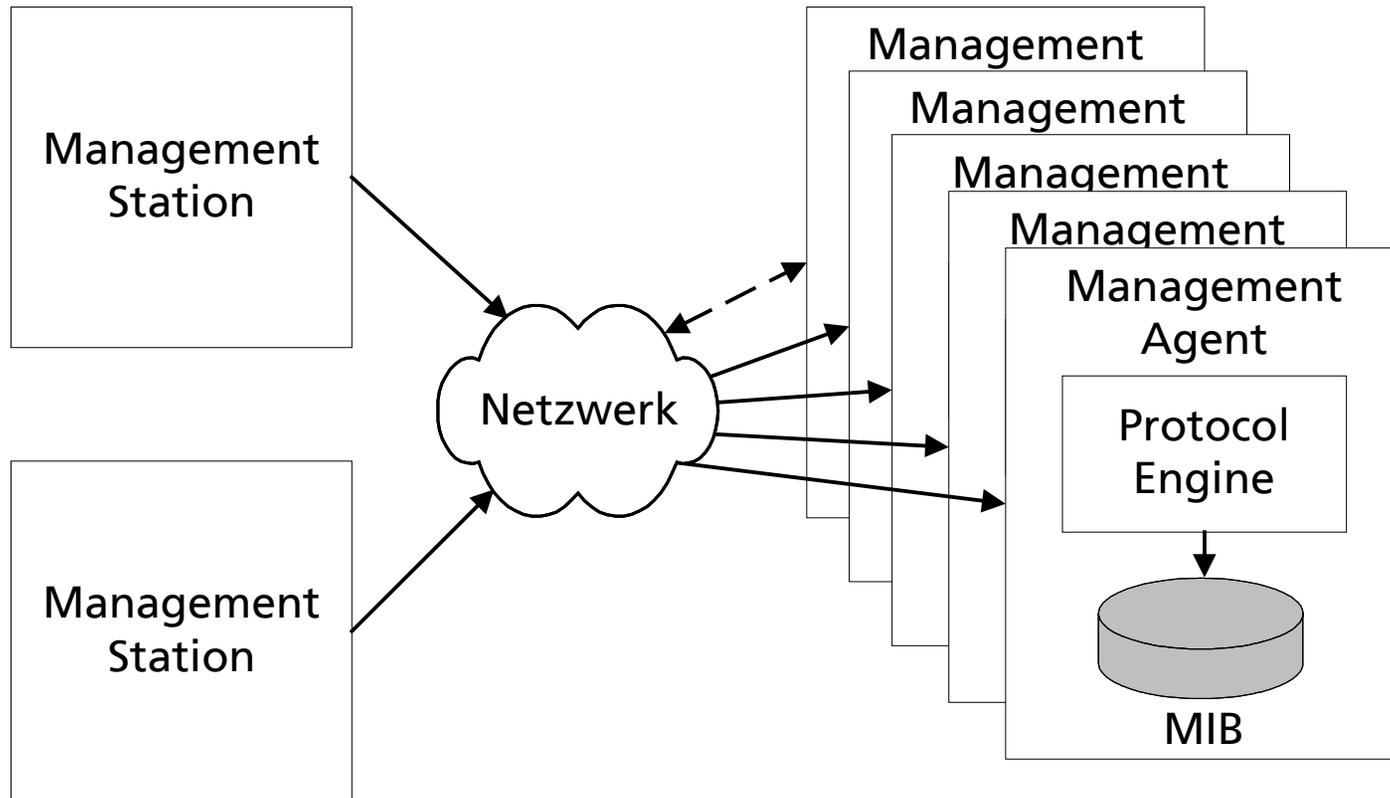
- Aufgaben, die SNMP erfüllen soll:
 - Erstellung von Statistiken, Datenanalyse, Visualisierung
 - Interaktive Schnittstelle zur Überwachung des Netzwerks
 - Automatische Heuristiken zur Fehleridentifikation
 - Sammlung von Daten zur automatischen Bestandspflege





Interaktionen der Architekturkomponenten

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Rollenverteilung

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Management Stations (meist nur eine) verwalten Management Agents. Agents reagieren auf Anfragen, können aber auch bei Ausnahmesituationen selbst asynchron Nachrichten versenden
- Zu verwaltende Ressourcen werden in MIBs zusammengefaßt.
- Protokollprimitive:
- `get` Abfrage der MIB-Objekte eines Agents durch eine Station
- `getnext` Lineare Abfrage mehrerer MIB-Objekte
- `set` Setzen von MIB-Objekten durch eine Station
- `trap` Asynchrone Benachrichtigung des Station durch Agenten





Standardisierung von „S“MNP

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

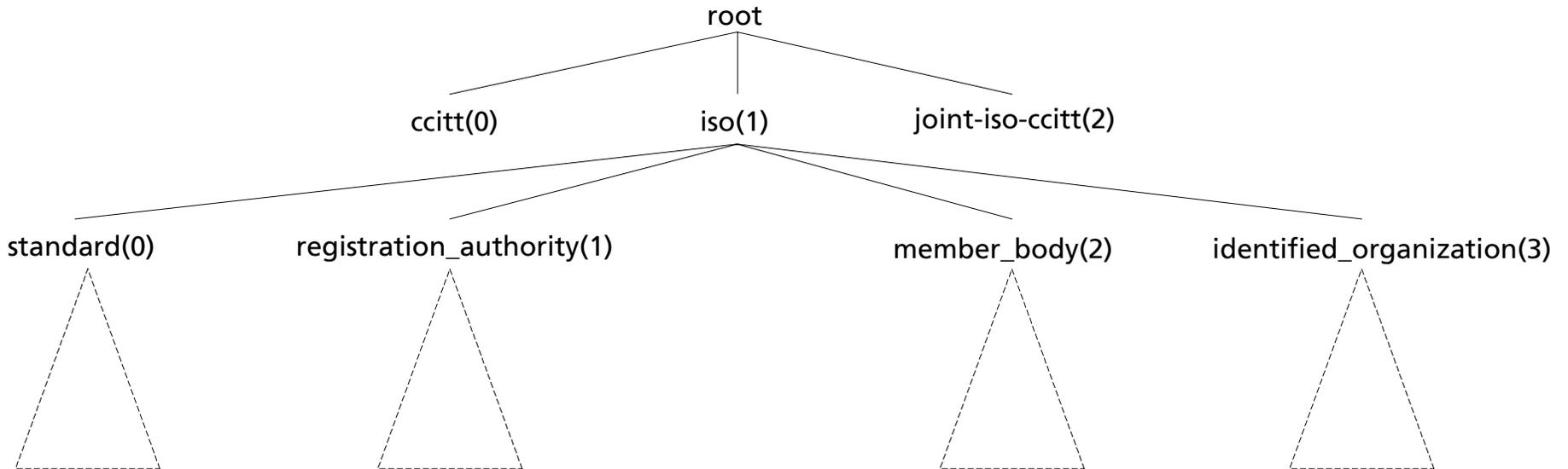
- SNMP besteht aus einer großen Anzahl von Teilstandards und Vorschlägen
- Aufgrund der Entscheidung zur Kompatibilität mit CMOT/OSI ist die MIB-Struktur unter Verwendung von ASN.1 realisiert
 - Hierarchische Anordnung von Object Identifiers (OIDs)
 - Weltweit eindeutige Zuordnung
 - ▲ Recht zur Zuteilung von OIDs wird entlang der Hierarchie delegiert
 - ▲ OIDs können als Pfad entlang eines Baumes dargestellt werden; numerische Codierung z.B. 1.1.5.3....





Partieller OID/MIB-Baum

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





Identifikation und Authentisierung in SNMPv1

... department security technology ... department security technology ... department security technology ... department security technology ...

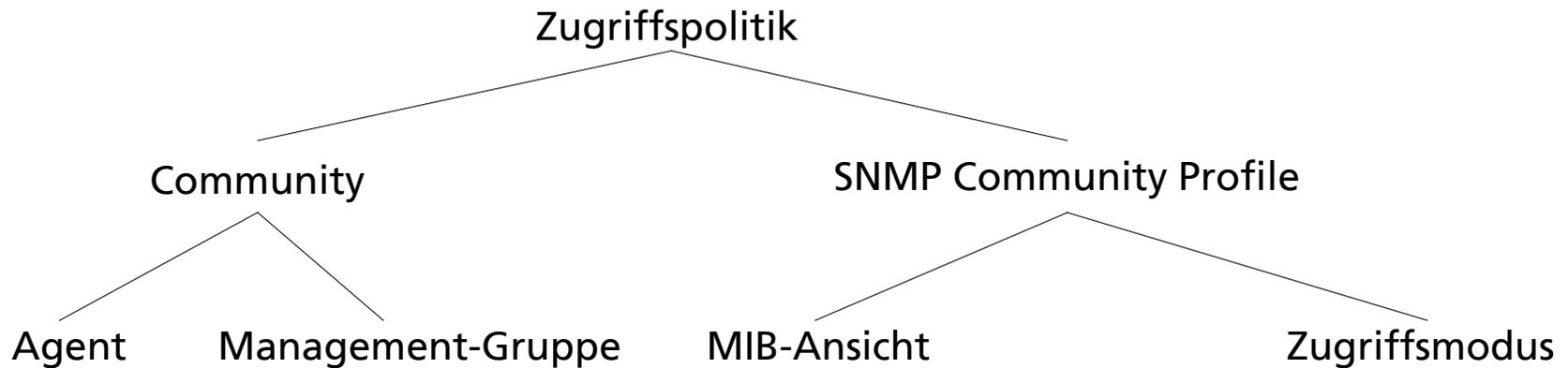
- I&A sind in SNMPv1 nur rudimentär vorhanden
- „Community“ definiert Authentisierung, Zugriffskontrolle, Proxy-Verhalten: über eindeutigen Namen identifiziert
- Konfiguration eines Management Agent erlaubt Bereitstellung unterschiedlicher Sichten für verschiedene Management Stations
 - Ableitung eines MIB-Views (vgl. View in RDBMS), kann für jede Community verschieden sein
 - Zugriffsmodus (READ-ONLY oder READ-WRITE)
- Abgleich der Zugriffsregeln mit ACCESS-Kategorien einer MIB erfolgt über ein Regelwerk





Administrative Konzepte in SNMPv1

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





SNMP-Zugriffsmodi

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

A C C E S S - K a t e g o r i e	Z u g r i f f s m o d u s	
r e a d o n l y	R E A D - O N L Y	R E A D - W R I T E
r e a d / w r i t e	V e r f ü g b a r f ü r g e t u n d t r a p	V e r f ü g b a r f ü r g e t , s e t u n d t r a p
W r i t e o n l y	V e r f ü g b a r f ü r g e t u n d t r a p	V e r f ü g b a r f ü r g e t , s e t u n d t r a p
N i c h t z u g r e i f b a r	N i c h t v e r f ü g b a r	





Probleme bei SNMPv1

... department security technology ... department security technology ... department security technology ... department security technology ...

- Die Zugriffssteuerung erfolgt ausschließlich über die Community-Strings im Klartext
 - Häufig werden sogar Hersteller-Standardwerte genutzt
 - Write-Community-Strings werden von manchen Geräten in Read-Community mit ausgegeben
- Wie syslog UDP-basiert (Port 161, 162):
Nachrichtenverluste
- MIBs sind zu komplex und dennoch unscharf genug, um herstellerspezifische Varianten für Management Stations zu erfordern
 - Komplexität von OSI wird als Ballast mitgeführt





SNMPv2

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Weiterentwicklung wurde 1992 begonnen als Reaktion auf
 - die bekannten Schwächen von SNMPv1
 - die fehlende Migration auf OSI-Protokolle

- Parallel dazu wurde 1992 ein neues Protokoll, SMP, entworfen
 - Möglichkeit zur Verwaltung beliebiger Ressourcen
 - ▲ Nicht nur Netzwerk-Ressourcen, auch Anwendungen, Hosts
 - ▲ Abfrage der Konformanz von Implementierungen
 - Mechanismus für Massendaten-Transfer
 - Sicherheitsmechanismen
 - Lauffähigkeit sowohl auf TCP/IP als auch auf OSI-Netzen





Schwierigkeiten bei der Entwicklung von SNMPv2 (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- SNMPv2 sollte als große Lösung auf Grundlage von SMP entwickelt werden: SMP wurde dazu umbenannt
- Die Komplexität von SNMPv2 war im gesetzten Zeitrahmen (bis Ende 1992) nicht vollständig zu beherrschen
 - Sicherheitsmechanismen fehlten in dieser Version völlig
- Definition einer „party“ (Sammlung von Ressourcen, Eigenschaften)
 - Informationen zu Transportmechanismen
 - clocks: Erkennung/Verhinderungen von Wiedereinspielungen
 - keys: Authentisierung/Verschlüsselung von Nachrichten
 - Zugriffsrechte, Operationen auf Views





Schwierigkeiten bei der Entwicklung von SNMPv2 (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Party-Konzept: Mächtig, aber nicht skalierbar
 - n^2 zu konfigurierende Relationen zwischen Management Agents, Stations im ungünstigsten Fall
 - Vorschlag zur Reduktion (user-Konzept, $O(n)$) wurde verworfen
- Reparatur des Modells durch SNMPv2-Arbeitsgruppe
 - Ebenfalls user-Konzept, dynamische Erzeugung und Löschung von parties
- Weitere interne Querelen und Spaltung innerhalb der Arbeitsgruppe sorgten für Scheitern von SNMPv2





SNMP Version 3

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- 1997 wurde erneut versucht, eine verwendbare SNMP-Erweiterung zu entwickeln: Neue IETF-Arbeitsgruppe SNMPv3
 - Wiederverwendung brauchbarer Konzepte aus SNMPv2
 - ▲ MIBs wurden nur um sicherheitsrelevante Elemente ergänzt
 - Hinzufügung von Sicherheitsmechanismen
 - Implementierungen sollten von minimaler Funktionalität bis zur vollen Realisierung machbar sein
 - Reduzierung von Querabhängigkeiten innerhalb des Standards





Module in SNMPv3-Komponenten (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Dispatcher
 - ermöglicht parallele Unterstützung mehrerer SNMP-Versionen, verteilt Nachrichten von/an Teilmodule
- Message Processing Subsystem
 - Präpariert Nachrichten für den Versand, extrahiert Nutzlast aus empfangenen Nachrichten
- Security Subsystem
 - Dienste für Vertraulichkeit, Authentisierung
- Access Control Subsystem
 - Dienste für Authorisierung, Verifikation von Zugriffsrechten





Module in SNMPv3-Komponenten (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

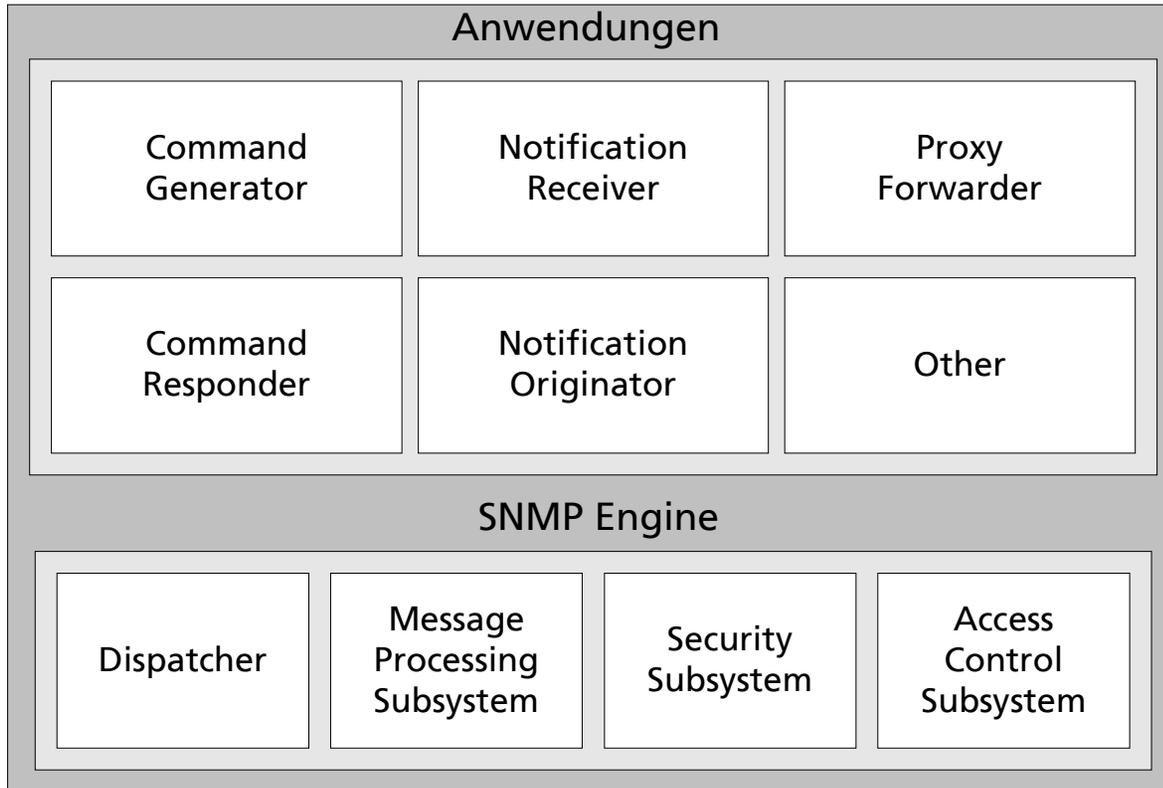
- **Command Generator**
 - Erzeugung der SNMP Protocol Data Units
- **Command Responder**
 - Empfang und Decodierung der für das lokale System bestimmten PDUs
- **Notification Originator**
 - Überwacht System auf bestimmte Ereignisse, erzeugt trap- oder inform-Ereignisse
- **Notification Receiver**
 - Lauscht auf Benachrichtigungen, erzeugt Bestätigungen für inform-Ereignisse
- **Proxy Forwarder**
 - Weiterleitung von Nachrichten





Modell einer SNMPv3-Komponente

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••





RMON

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Protokoll zur Sammlung und Weiterleitung von Management-Daten, insbesondere SNMP bestehend aus
 - RMON Probes (Sammeleinheiten)
 - RMON Console Managers (Administration/Darstellung)
 - Probes agieren als Konsolidierungsinstanzen in weit verteilten Netzwerken

- RMON faßt Daten in Monitoring-Gruppen zusammen
 - ▲ Netzwerk-Statistiken, unabhängige Bestimmung von Alarmwerten, Host-Statistiken, Packet Capture, Filterregeln für Packet Capture, Ereignisse...





Windows NT Event Log (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Client/Server-System

- Event-Dienst ist als System Service konfiguriert
- Verwaltung, Konfiguration erfolgt über eine separate Anwendung: Event Viewer. Dieser erlaubt
 - ▲ Festlegung maximaler Speicherplatz
 - ▲ Vorgehen für Sicherung von Log-Dateien
 - ▲ Ansicht und einfache Filter der Revisionsdaten
- Lokaler Zugriff über LPC
- Entfernter Zugriff via (MS) RPC möglich
- Kategorien: „Information“, „Warning“, „Error“





Windows NT Event Log (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Event Log ist in drei Teil-Logs unterteilt

- Application Log
 - ▲ Jede registrierte Anwendung kann dorthin schreiben
 - ▲ Übersetzung zwischen Codes, Text über Message-Datei
- Security Log
 - ▲ Nur NT-Revisionsmechanismen (SRM, Drucksystem, WinLogon...) haben Zugriff
 - ▲ Anmeldevorgänge werden nur auf lokalem System protokolliert
- System Log
 - ▲ Nur System-Komponenten (Netzwerk-Subsystem...)





Tripwire (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- 1992 von Kim und Spafford am COAST entwickelt
- Schützt die Integrität von Dateisystemen, Router-Konfigurationen vor unbefugten Modifikationen
- Berechnet kryptographische Hashwerte der zu schützenden Dateien und speichert diese in Datenbank
 - Erlaubt Sicherung einer bekannt funktionstüchtigen, vertrauenswürdigen und abgenommenen Konfiguration
 - Vergleich der Hash-Werte auf nicht überschreibbarem Medium mit Ist-Wert
 - Erkennung von neuen, gelöschten Dateien





Tripwire (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Wurde kommerzialisiert, ist auf verschiedenen Plattformen verfügbar
 - Umfangreiche Analyse- und Berichtsmöglichkeiten, zentrale Verwaltung und Überwachung der Tripwire-Datenbanken in Netzwerken

- Andere Werkzeuge mit ähnlichen Funktionen
 - Hobgoblin
 - AIDE
 - ATP
 - Tripwire / Open Source (Linux, FreeBSD)





Protokollierungs-Architekturen

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Gesamte Prozeßkette von Erzeugung bis zur Archivierung muß berücksichtigt werden
- Speicherung auf Firewall-Knoten ist nicht sinnvoll
 - Single Point of Failure
 - Bei Kompromittierung der Firewall gehen Revisionsdaten verloren oder werden unglaubwürdig
 - ▲ keine forensische Analyse mehr möglich
 - Zerstörung der Revisionsdaten kann auch durch andere Fehlfunktionen induziert werden





Anforderungen an Protokollierungs-Architekturen (1)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

- Daten müssen derart gesichert werden, daß
 - Ursprung zweifelsfrei nachgewiesen werden kann
 - Integrität der Daten zwischen Entstehungsort und Speicherungsart verifizierbar nicht beeinträchtigt ist
 - Fehlverhalten einer Quelle sich ausschließlich auf Daten auswirken, die nach Eintritt der Fehlerbedingung erzeugt werden
 - Zumindest innerhalb der Daten einer Quelle eine Ordnungsrelation auf Protokolldaten-Elementen realisiert ist





Anforderungen an Protokollierungs-Architekturen (2)

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Weitere Forderungen

- Vertraulichkeit, Zugriffskontrolle von übertragenen, archivierten Daten: Bestimmt durch Sicherheitspolitik
- Wohldefiniertes Verhalten bei Versagen der Protokollierungs-Mechanismen: Anhalten oder Verlust der Daten akzeptieren

■ Die vorgestellten Revisionsmechanismen basieren sämtlich auf UDP, Meldungen können in erheblichem Umfang verloren gehen

- Verwendung separater Administrationsnetzwerke ist sinnvoll, löst Problem aber nicht vollständig





Vermeidung von Nachrichtenverlusten

••• department security technology ••• department security technology ••• department security technology ••• department security technology •••

■ Anforderungen

- Blockierende Semantik für Nachrichtenübertragung
- Unabhängigkeit von übrigem Netzwerkverkehr
- Punkt-zu-Punkt Verbindung (Switches und andere Infrastruktur-Komponenten können ebenfalls kompromittiert oder deaktiviert werden)

■ Serielle Verbindungen zu separatem Log-Host ohne Verbindung mit geschütztem Netzwerk

- Konsolidierung mittels Systemen wie dem VAXCluster Console System (jetzt: CA Unicenter Console Management)

