NET311
Computer Network Management
SNMPv3

Dr. Mostafa H. Dahshan
Department of Computer Engineering
College of Computer and Information Sciences
King Saud University
mdahshan@ksu.edu.sa

Acknowledgements

- Notes are based on slides of:
  - Network Management: Principles and Practice, 2E, Mani Subramanian.

SNMPv3 Key Features

- Modularization of document
- Modularization of architecture
- SNMP engine
- Security features

SNMPv3 Architecture

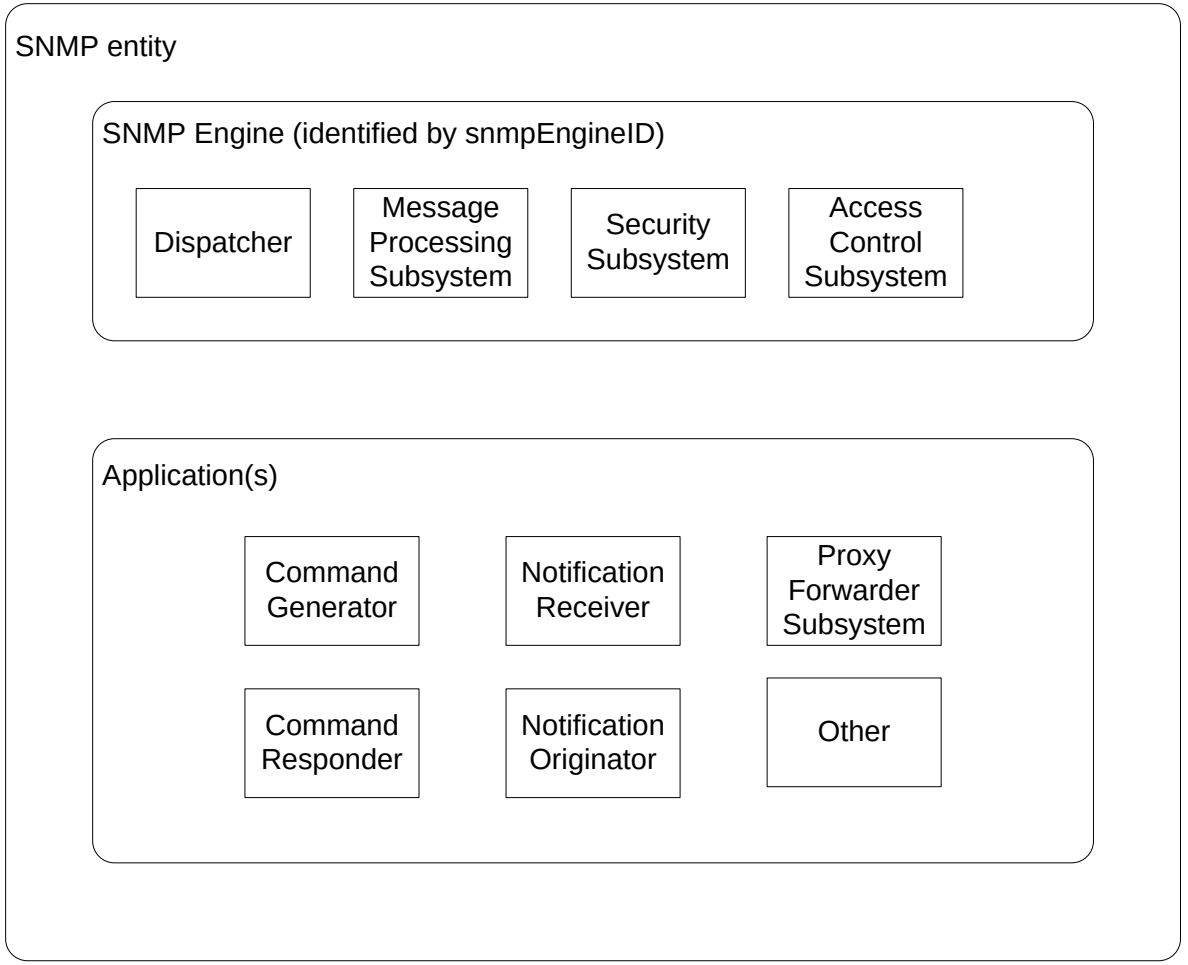

Figure 7.2 SNMPv3 Architecture

SNMPv3 Architecture

- SNMP entity is a node with an SNMP management element
- Either an agent or manager or both
- Three names associated with an entity
  - Entities: SNMP engine
  - Identities: Principal and security name
  - Management Information: Context engine

SNMP Engine ID

- Each SNMP engine has a unique ID: snmpEngineID
- Acme Networks {enterprises 696}
- SNMPv1 snmpEngineID ‘000002b8’H
- SNMPv3 snmpEngineID ‘800002b8’H (the 1st octet is 1000 0000)

- Engine ID is used with hash function to generate keys for authentication and encryption

SNMPv3 Engine ID

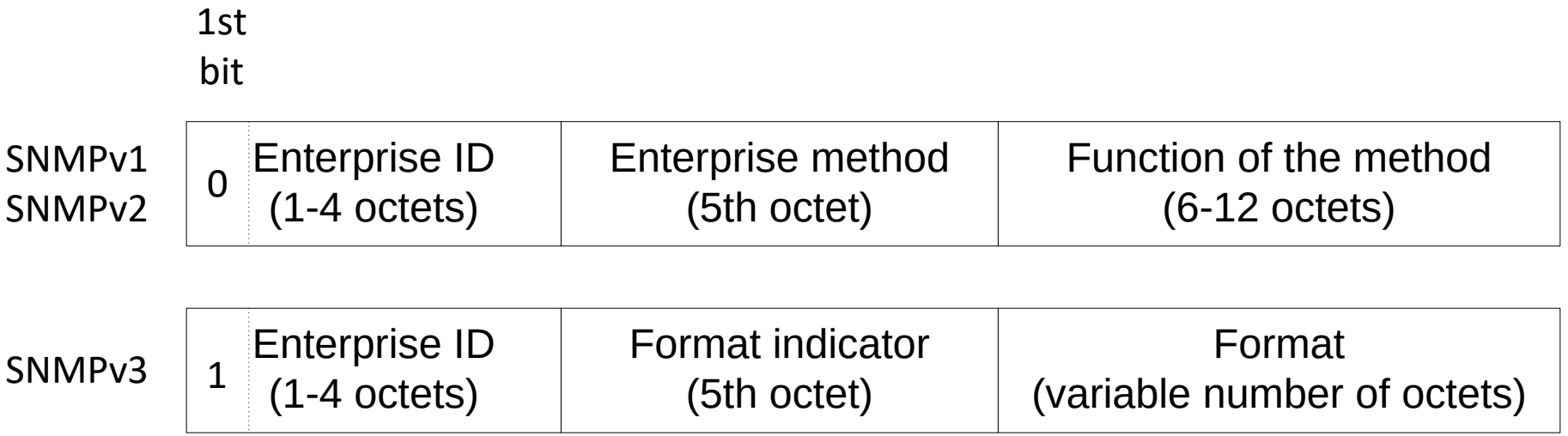

Figure 7.3 SNMP Engine ID

SNMPv3 Engine ID

Table 7.2 SNMPv3 Engine ID Format (5th octet)

Value	Description
0	Reserved, unused
1	IPv4 address (4 octets)
2	IPv6 (16 octets) Lowest non-special IP address
3	MAC address (6 octets) Lowest IEEE MAC address, canonical order
4	Text, administratively assigned Maximum remaining length 27
5	Octets, administratively assigned Maximum remaining length 27
6-127	Reserved, unused

SNMPv3 Engine ID

- For SNMPv1 and SNMPv2:
- Octet 5 is the method
- Octet 6-12 is IP address
- Examples
  - IBM host IP address 10.10.10.10
  - SNMPv1: 00 00 00 02 01 0A 0A 0A 0A 00 00 00
  - SNMPv3: 10 00 00 02 02 00 00 ... 00 00 00 0A 0A 0A 0A

SNMPv3 MIB

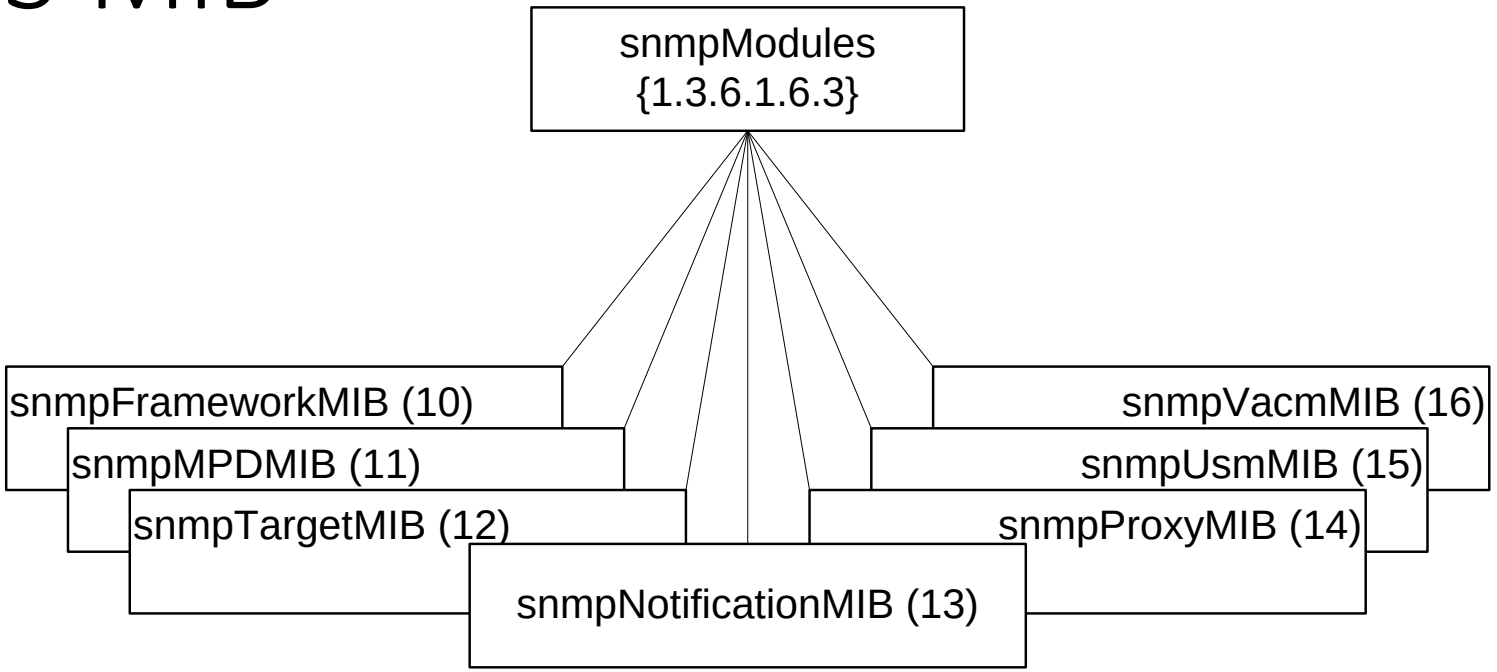

Figure 7.7 SNMPv3 MIB

Notes

- SNMPv3 MIB developed under snmpModules
- SNMPv2 Security placeholder is not used

SNMPv3 MIB

MIB	Description
snmpFrameworkMIB	describes SNMP management architecture
snmpMPDMIB	identifies objects in the message processing and dispatch subsystems
snmpTargetMIB snmpNotificationMIB	used for notification generation
snmpProxyMIB	defines translation table for proxy forwarding
snmpUsm MIB	defines user-based security model objects
snmpVacmMIB	defines objects for view-based access control

Security Threats

- Modification of information
  - Contents modified by unauthorized user, does not include address change
- Masquerade
  - message altered by an unauthorized user
  - change of originating address
  - fragments of message altered to modify the meaning of the message
- Disclosure
  - eavesdropping
  - does not require interception of message

Security Threats

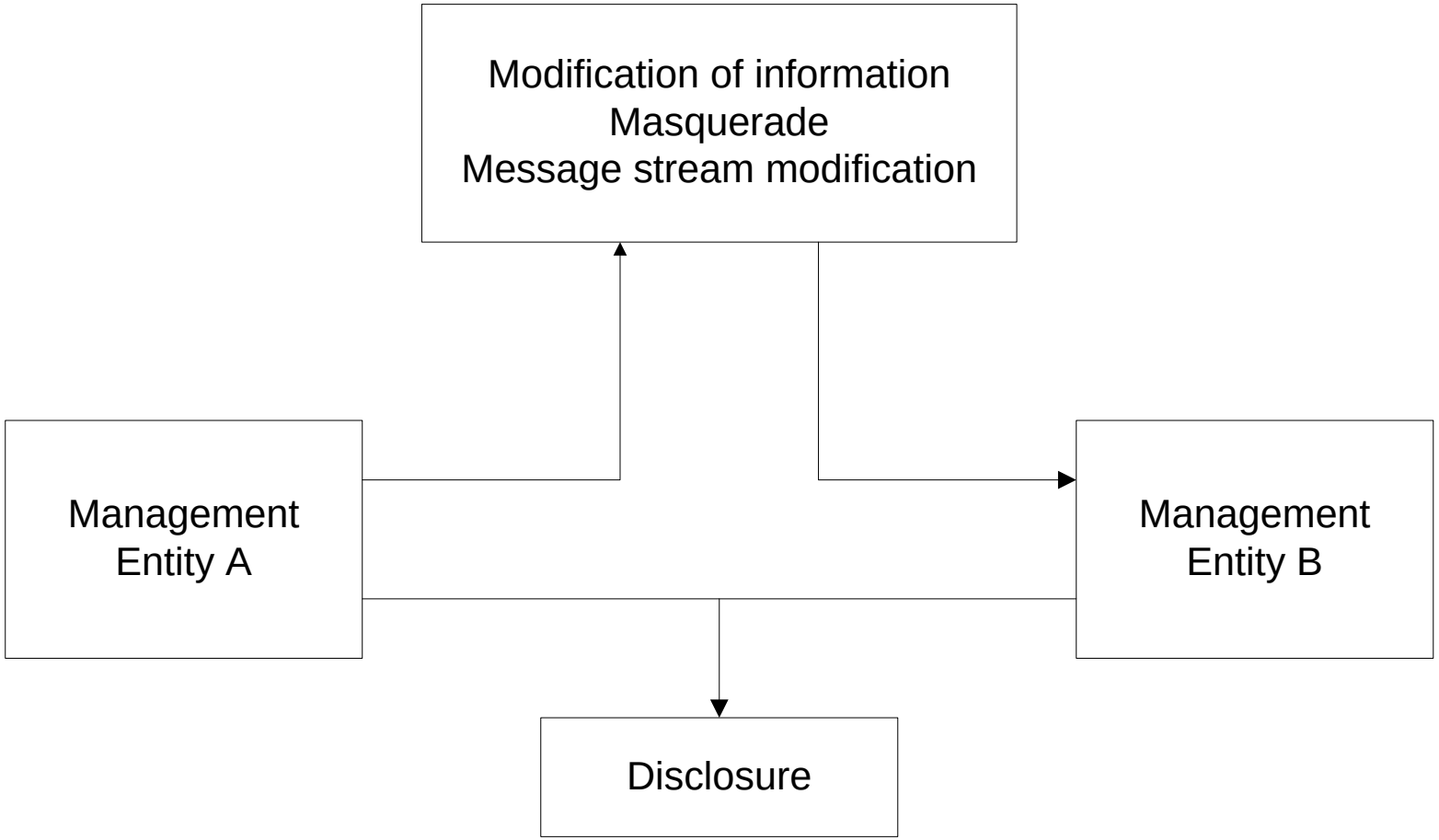

Figure 7.10 Security Threats to Management Information

Security Services

- Data integrity
  - HMAC-MD5-96 / HMAC-SHA-96
- Data origin authentication
  - Append a unique Identifier associated with authoritative SNMP engine
- Privacy / confidentiality
  - Encryption
- Timeliness
  - Authoritative Engine ID
  - Number of engine boots and time in seconds

Security Services

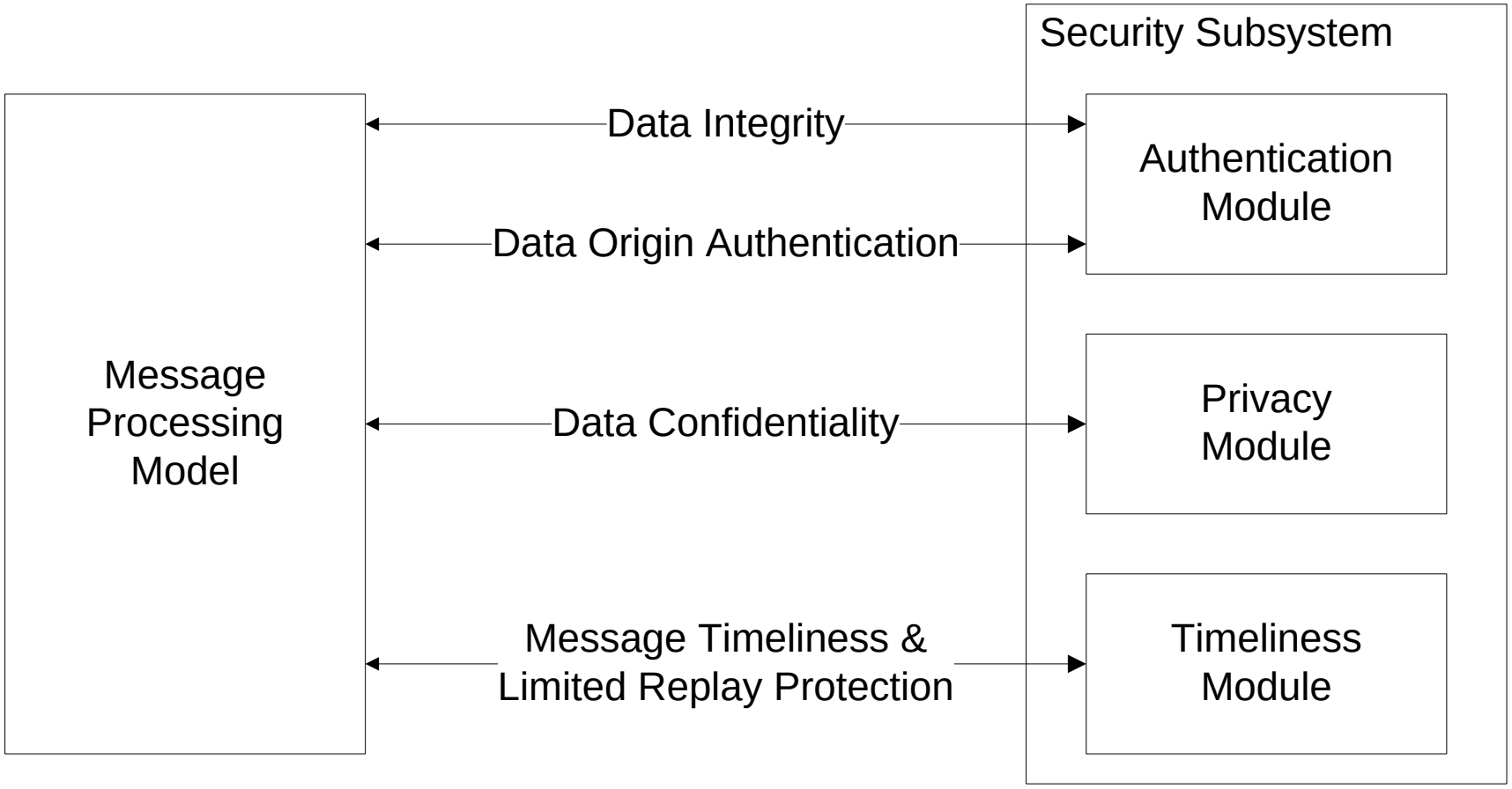

Figure 7.11 Security Services

User-based Security Model

- Based on traditional user name concept
- USM primitives across abstract service interfaces
- Authentication service primitives
  - authenticateOutgoingMsg
  - authenticateIncomingMsg
- Privacy Services
  - encryptData
  - decryptData

Secure Outgoing Message

- USM invokes privacy module with encryption key and scopedPDU
- Privacy module returns privacy parameters and encrypted scopedPDU
- USM invokes authentication module with authentication key and whole message
- USM receives authenticated whole message

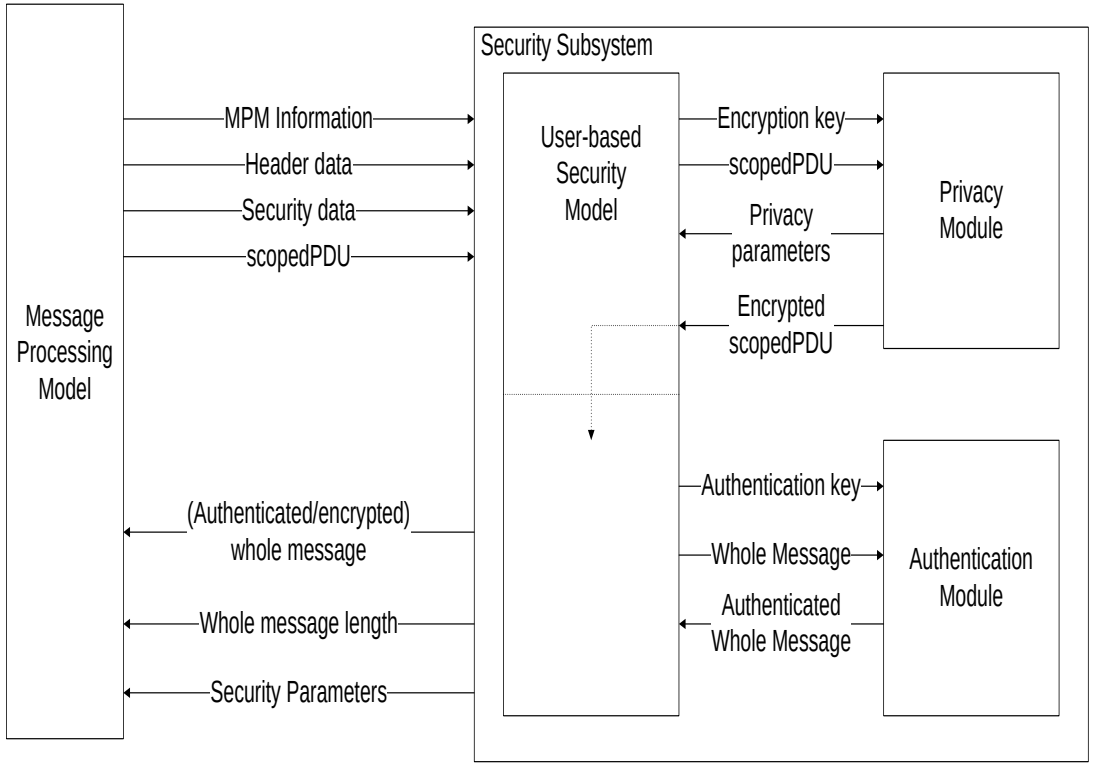

Figure 7.13 Privacy and Authentication Service for Outgoing Message

Secure Incoming Message

- Processing secure incoming message reverse of secure outgoing message
- Authentication validation done first by authentication module
- Decryption of message is then done by the privacy module

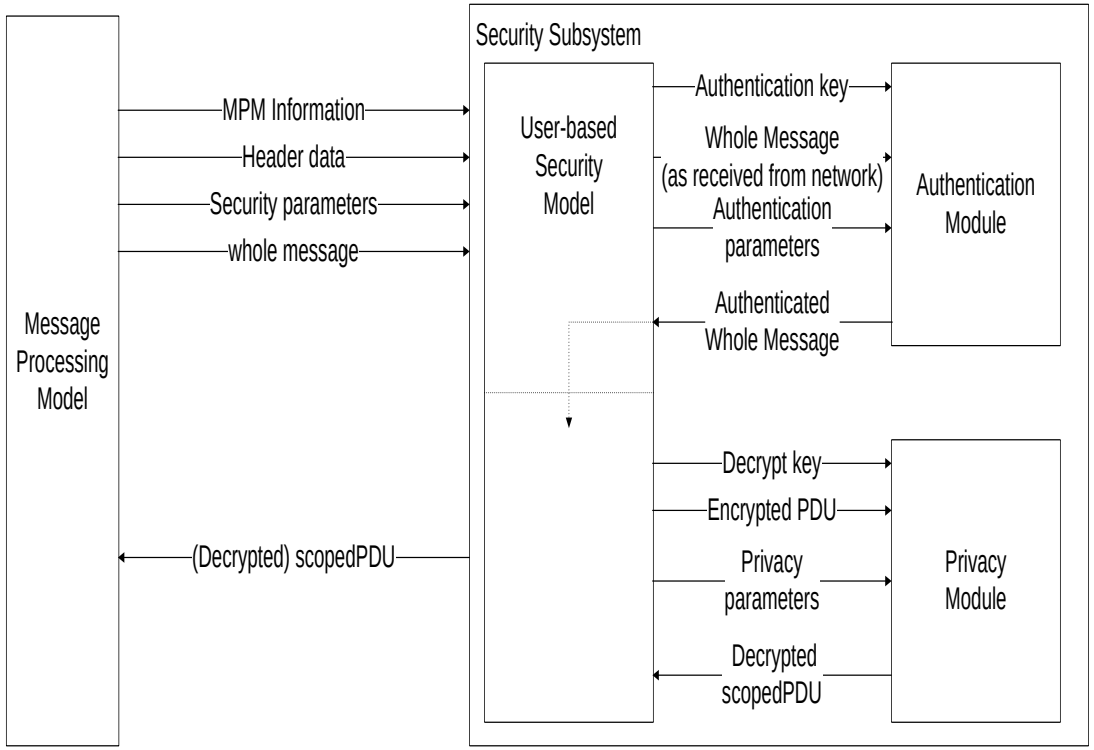

Figure 7.14 Privacy and Authentication Service for Incoming Message

Access Control

- View-based Access Control Model
- Groups
  - name of the group comprising security model and security name
  - in SNMPv1, group is community name
- Security Level
  - no authentication - no privacy
  - authentication - no privacy
  - authentication - privacy
- Contexts
  - names of the context

Access Control

- MIB Views and View Families
  - MIB view is a combination of view subtrees
- Access Policy
  - read-view
  - write-view
  - notify-view
  - not-accessible

VACM Process

Answers 6 questions:

1. Who are you (group)?
2. Where do you want to go (context)?
3. How secured are you to access the information (security model and security level)?
4. Why do you want to access the information (read, write, or send notification)?
5. What object (object type) do you want to access?
6. Which object (object instance) do you want to access?

VACM MIB

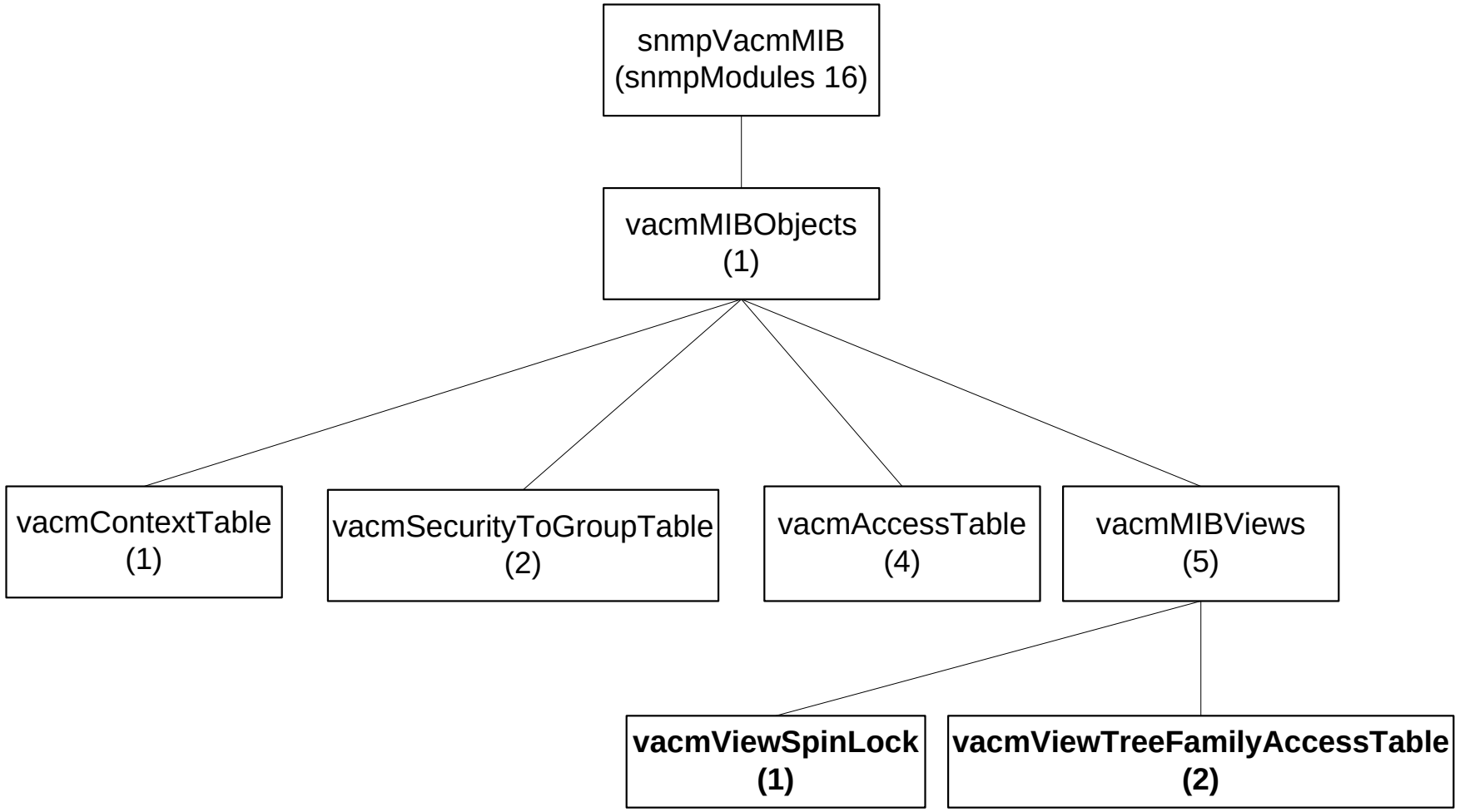

Figure 7.17 VACM MIB

MIB Views

- Simple view:
  - *system* 1.3.6.1.2.1.1
- Complex view:
  - all information relevant to a particular interface
  - *system* and *interfaces* groups
- Family view subtrees
  - view with all columnar objects in a row appear as separate subtree
  - OBJECT IDENTIFIER (family name) paired with bit-string value (family mask) to select or suppress columnar objects

VACM MIB View

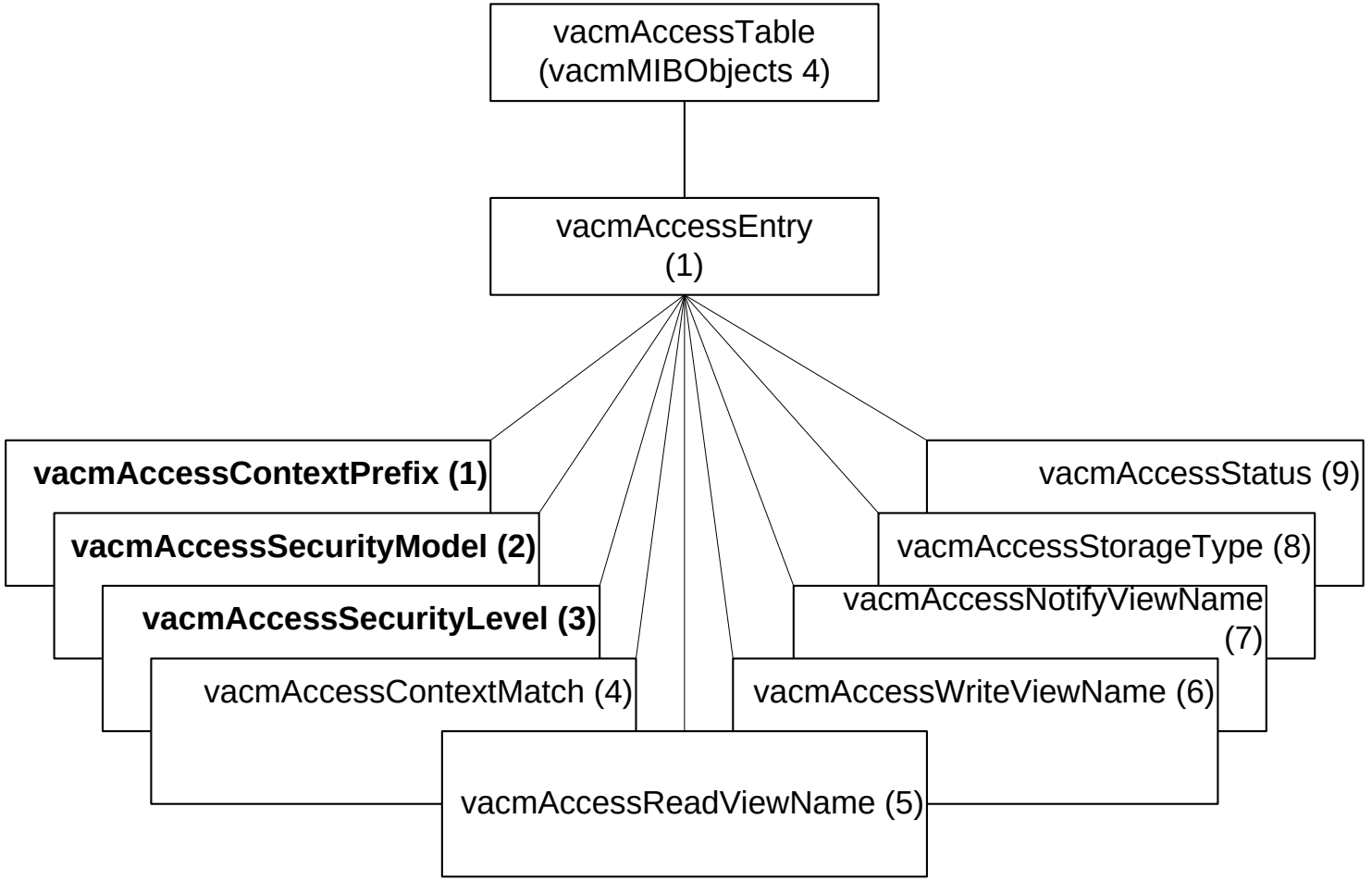

Figure 7.18 VACM Access Table

VACM MIB View Examples

- Family view name = “system”
- Family subtree = 1.3.6.1.2.1.1
- Family mask = “” (implies all 1s by convention)
- Family type = 1 (implies value to be included)

- More examples are available in the tutorial