Application Layer: SNMP;SSL

Dr. G. Omprakash

Assistant Professor, ECE, KLEF

Aim of the session

To familiarize the students with the basic concept of the socket, Secure Socket Layer, and the working of the simple mail transfer protocol

Learning Outcomes

At the end of this session, you should be able to:

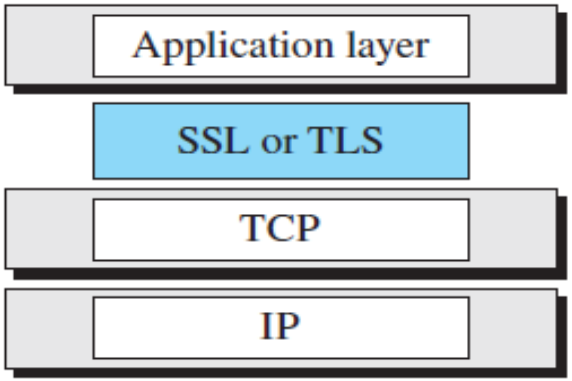
- Describe the Secure Socket Layer and
- Describe the working of simple mail transfer protocol

Overview

Secure Socket Layer (SSL) Protocol

Transport Layer Security

- Security at the transport layer provides security for the application layer
- Before the messages are encapsulated in TCP, they are encapsulated in the security protocol packets.
- Two protocols are dominant today for providing security at the transport layer
  - Secure Sockets Layer (SSL) Protocol
  - Transport Layer Security (TLS) Protocol (IETF version of SSL)
- Goals of these protocols is to provide: server and client authentication, data confidentiality, and data integrity



SSL Protocol Suite

SSL is designed to provide security and compression services to data generated from the application layer

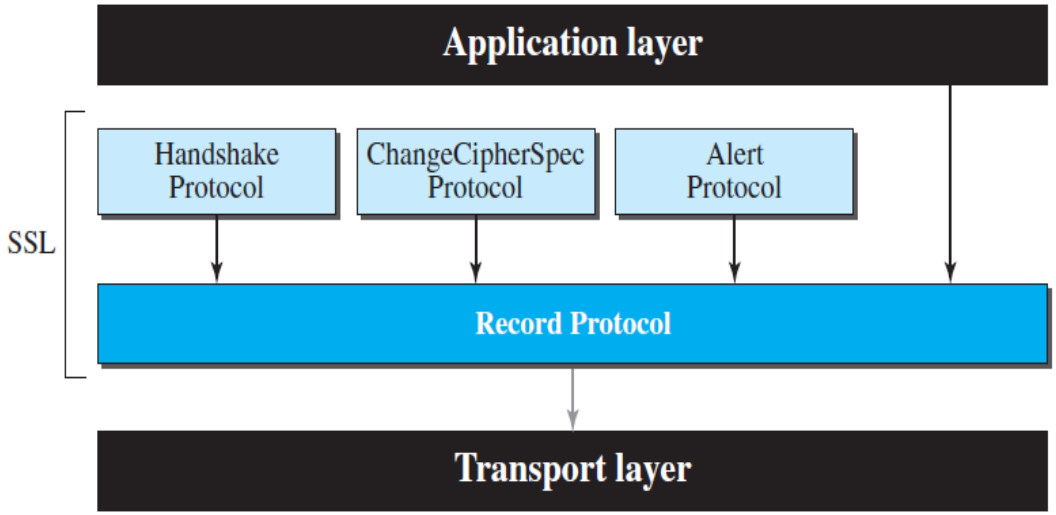


Figure: Four SSL protocols

SSL Protocol Suite

- **Record Protocol**: It carries messages from three other protocols as well as the data coming from the application layer. (**Carrier**)
- **Handshake Protocol**: provides security parameters for the Record Protocol
  - Provides keys and cipher set
  - Authenticates the server to the client and vice-versa
- **ChangeCipherSpec Protocol** is used for signaling the readiness of cryptographic secrets.
  - The sender and the receiver need two states
  - Pending state: Keeps track of the parameters and secrets
  - Active state: parameters and secrets used by the Record Protocol to sign/verify or encrypt/decrypt messages
- **Alert Protocol** is used to report abnormal conditions and reporting errors.

Handshake Protocol

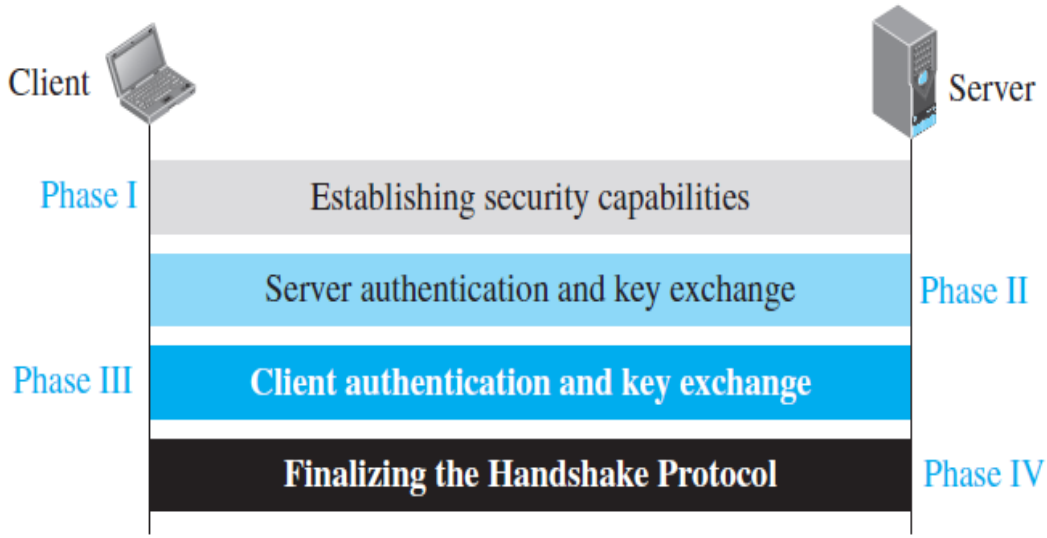


Figure: Handshake protocol

Processing done by record protocol

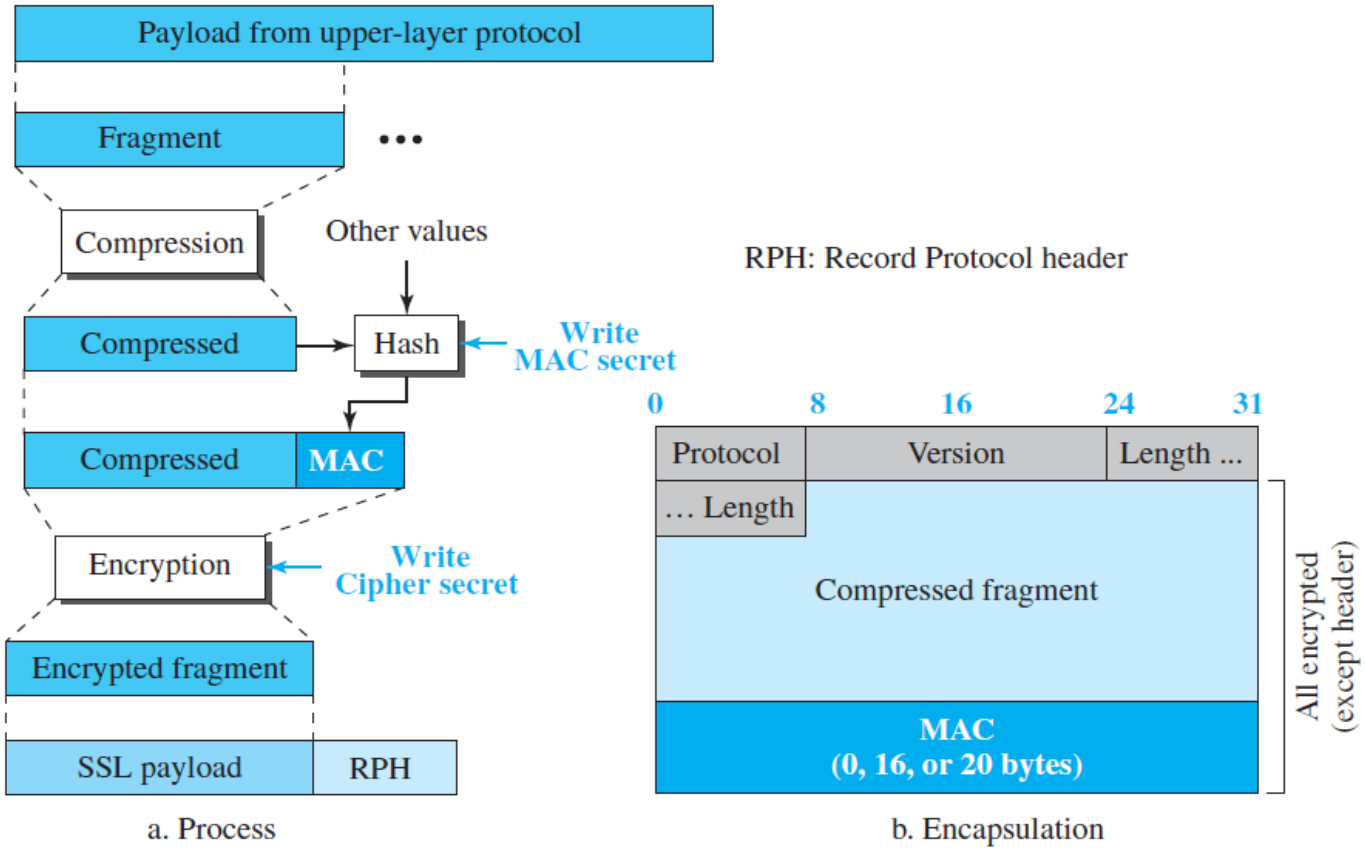


Figure: Processing done by the Record Protocol

Processing done by record protocol

- The Record Protocol carries messages from the upper layer
- The message is fragmented and optionally compressed
- A MAC is added to the compressed message using the negotiated hash algorithm
  - SSL uses hash algorithms to provide message integrity (authentication)
- The compressed fragment and the MAC are encrypted using the negotiated encryption algorithm
- Finally, the SSL header is added to the encrypted message.

Simple Network Management Protocol

Network Management

- Network management is implemented at the application layer of the TCP/ IP protocol suite
- The failure of a single device may interrupt the communication from one point of the Internet to the other

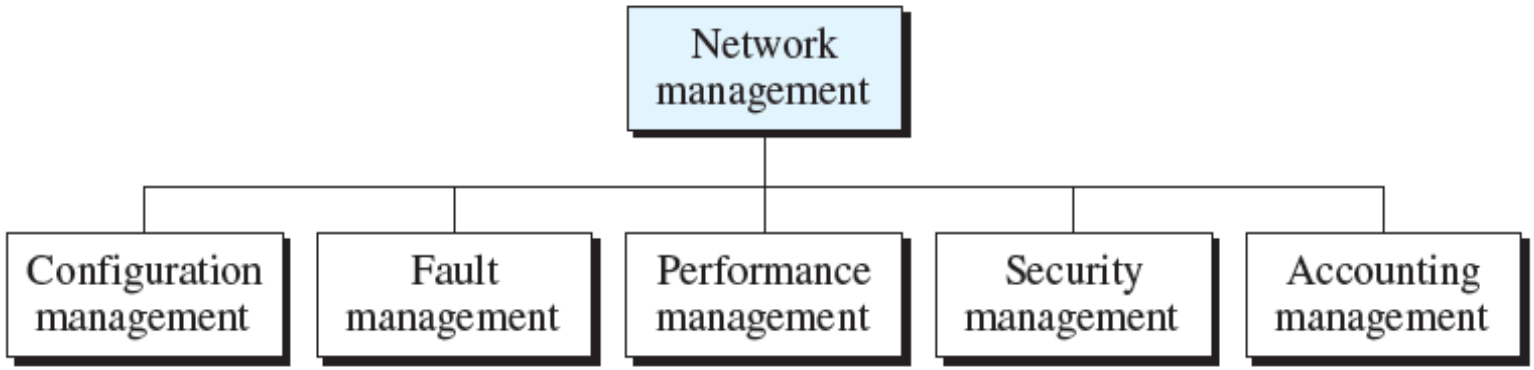


Figure: Areas of network management

Network Management

- **Configuration Management**: system must know, at any time, the status of each entity and its relation to other entities
- Configuration management is divided into *reconfiguration* and *documentation*
  - **Reconfiguration**: Hardware reconfiguration, software reconfiguration, and user account reconfiguration.
    - Replacing route (Updating MAC Address)
  - **Documentation**: The original network configuration and each subsequent change must be recorded meticulously
  - Network relation (maps), specifications

Network Management

- **Fault Management**: takes care of proper operation of each component
  - Two subsystems: reactive fault management and proactive fault management.
  - **Reactive fault management**: Detecting, isolating, correcting faults
  - **Proactive fault management**: tries to prevent faults from occurring
    - Based on lifetime of components -replace them
- **Performance Management**: tries to monitor and control the network to ensure that it is running as efficiently as possible
  - Capacity, Traffic, Throughput, Response time

Network Management

- **Security Management**: responsible for controlling access to the network
  - Encryption allows privacy for users
  - Authentication forces the users to identify themselves.
- **Accounting Management**: is the controlling of users' access to network resources through charges.
  - It prevents users from monopolizing limited network resources
  - It prevents users from using the system inefficiently.

SNMP

- SNMP is a framework for managing devices in an internet using the TCP/IP protocol suite
- It provides a set of fundamental operations for monitoring and maintaining an internet.
- SNMP uses the concept of manager and agent.
- Manager (usually a host) controls and monitors a set of agents (usually routers or servers)

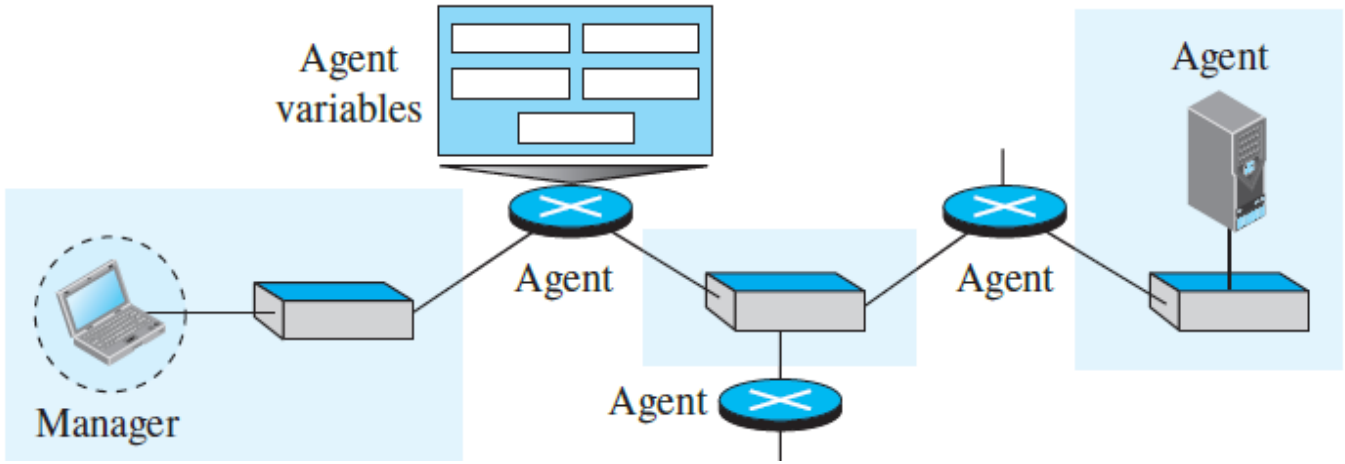


Figure: SNMP Concept

Components of SNMP

- SNMP uses two other protocols:
  - Structure of Management Information (SMI)
  - Management Information Base (MIB)

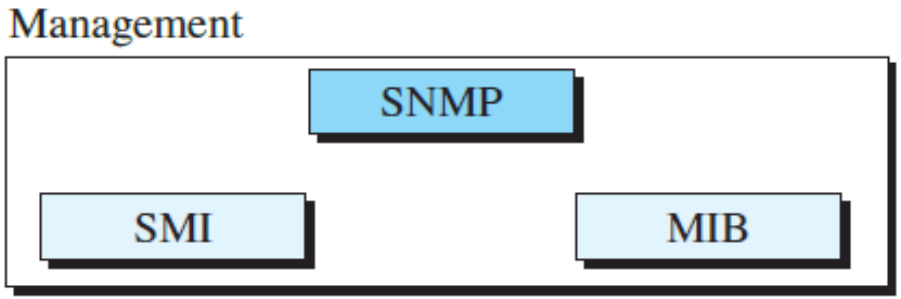


Figure: Components of SNMP

- **Role of SNMP**: It defines the format of the packet exchanged between a manager and an agent
- The packets exchanged contain the object (variable) names and their status (values).

Components of SNMP

- **Role of SMI**: SMI defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values
- **Role of MIB**: MIB creates a collection of named objects, their types, and their relationships to each other in an entity to be managed

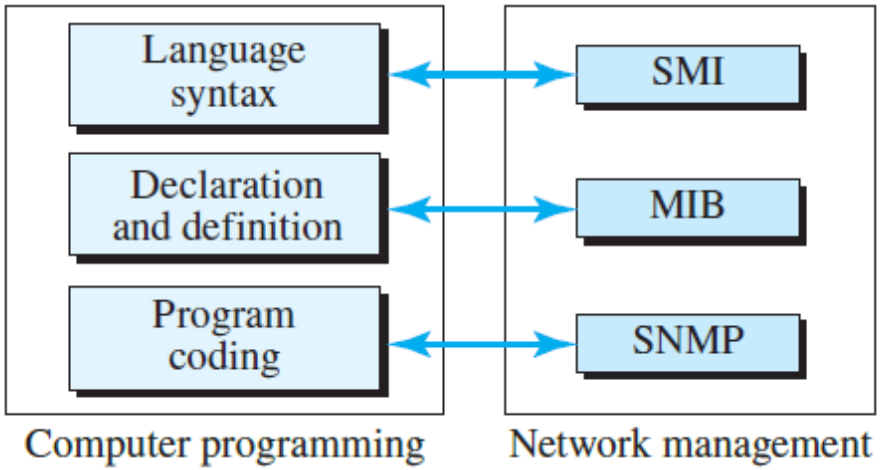


Figure: Comparing computer programming and network management

Overview Example

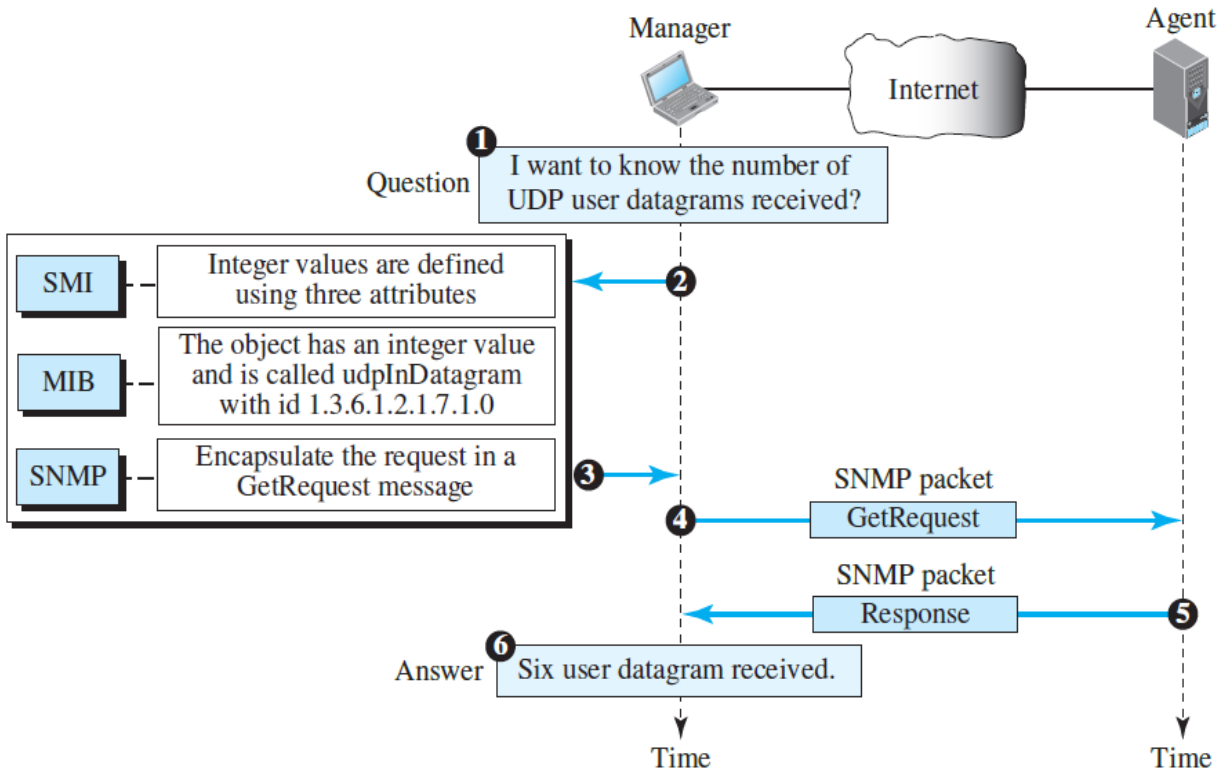


Figure: Management overview

Overview Example

- Manager (SNMP Client) wants to find the number of UDP datagrams received by the agent (SNMP server)
- SMI is responsible for encoding the name of the object
- SNMP is responsible for creating GetRequest message

Acknowledge various sources for the images.
Thankyou