NETWORK

SECURITY

04 INFORMATION ASSURANCE

Contents

4.1 Network Architecture

- To be able to implement security in a communications network, it is necessary to understand how the network operates.

- The term *computer network* is mostly used to describe several autonomous computers and servers interconnected in a complex structure (Tanenbaum, 1981).

4.1 Network Architecture

- Computer networks are organized in a series of layers or levels.

- The purpose of each layer is to offer certain services to higher layers and to shield them from the details of service implementation.

4.2 OSI and TCP/IP Model

4.2.1 OSI 7 Layers Reference Model

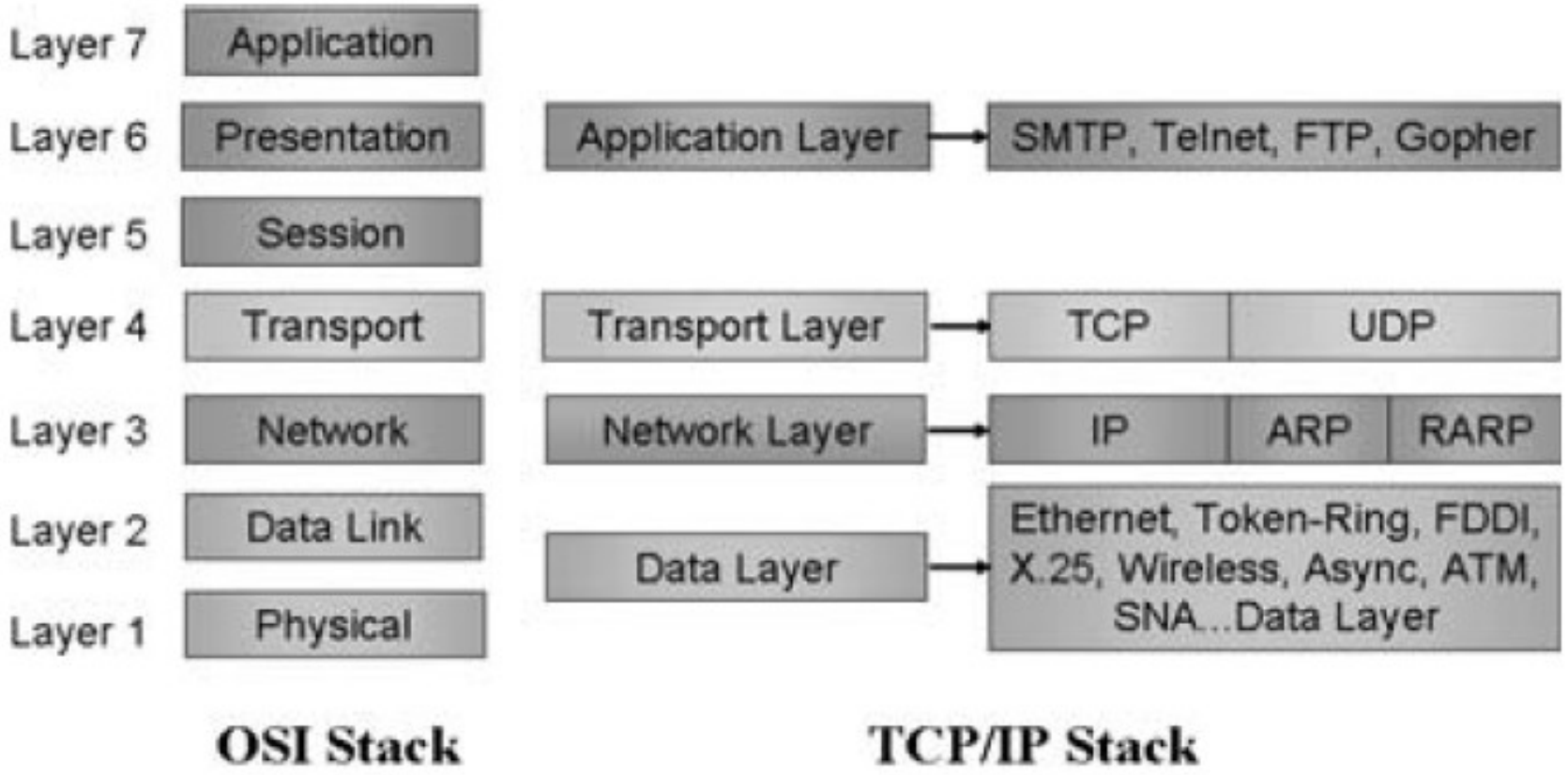
- The OSI divides communications into seven layers, each providing a specific set of services from a lower level.

- The ISO IEC 7498-3: 1997—basic reference model.

4.2 OSI and TCP/IP Model

- Each layer can be developed independently and is constrained only by the services it provides to the *n* + *1* layer and by the services provided by the *n* - *1* layer.

4.2 OSI and TCP/IP Model



4.2 OSI and TCP/IP Model

Application

- The application layer is where users process the information and determine which programs they will run and which protocols they will use.
- Simple mail transfer protocol (smtp), hypertext transfer protocol (http), file transfer protocol (ftp), telnet, and trivial transfer protocol (TFTP) are some examples of the protocols working at the application layer.

4.2 OSI and TCP/IP Model

Presentation

- The function of the presentation layer is to provide the users with certain useful, but not always essential, transformation services of the users' data.
- These services include conversion between character codes (8-bit ASCII, virtual terminal protocols), cryptographic transformations, text compression, terminal handling, file transfer, and manipulation of files.

4.2 OSI and TCP/IP Model

Session

- The session layer is the user's interface with the network.
- The user must negotiate with this layer to establish a connection with another machine.
- A connection between users (or between two presentation layers) is called a *session*.
- The network file system (NFS), structured query language (SQL), and remote procedure call (RPC) are some examples.

4.2 OSI and TCP/IP Model

Transport

- The transport layer's task is to provide reliable and efficient end-to-end transport service between users' processes.
- Collectively, layers 1 through 4 provide a transport service, shielding the higher layers from the technical details of how communication is achieved.

4.2 OSI and TCP/IP Model

Network

- The lowest three layers (3, 2, and 1) are concerned with the end-to-end transmission, framing, and routing of packets between machines.
- A network layer, sometimes called the communication subnet layer, controls the exchange of data between the user and the network, as well as the operation of the subnet.

4.2 OSI and TCP/IP Model

- The network layer groups the binary digits, including data and control elements, into packets of information composed of header, data, and trailer, which are transmitted as a whole.
- Internet protocol (IP), Internet control message protocol ICMP), routing information protocol (RIP), open shortest path first (OSPF), and border gateway protocol (BGP) are some examples of the protocols working at the network layer.

4.2 OSI and TCP/IP Model

Data Link

- When the packets from layer 3 arrive at layer 2, a frame header and trailer are attached for transmission.

- The data link layer breaks up the data from the network layer into data frames and transmits the frames sequentially.

4.2 OSI and TCP/IP Model

- Advanced data communication control (ADCCP), layer 2 forwarding (L2F), layer 2 tunneling protocol (L2TP), and high-level data control (HDLC), asynchronous transfer mode (ATM) are some examples of the protocols.

- All these protocols allow data frames to contain an arbitrary number of bits and are referred to as bit-oriented protocols.

4.2 OSI and TCP/IP Model

Physical

- The physical layer (layer 1) converts bits into electrical signals, and it is involved with the transmission and reception of the raw bits over a communication system.

- Integrated services digital network (ISDN), Ethernet physical layer, and SONET/SDH are some examples.

4.2 OSI and TCP/IP Model

- The main task of the physical layer is to make sure that when a 0 bit is sent, the other physical layer will receive a 0 bit and not a 1.

- Most of the time, the physical layer is connected to bridges, routers, switches, gateways, or modems.

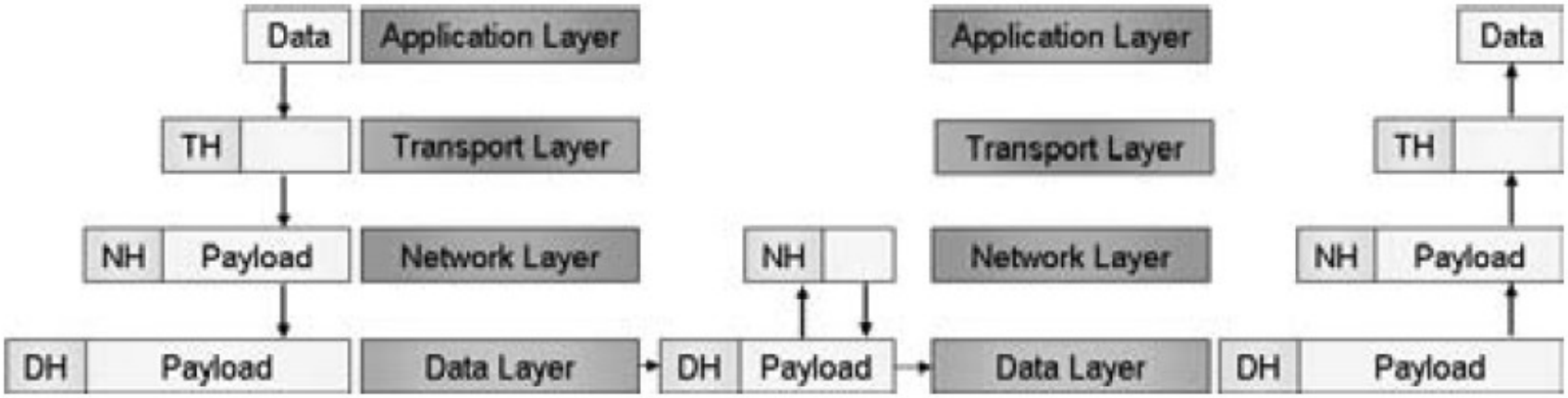
4.2 OSI and TCP/IP Model

4.2.2 TCP/IP Model

- TCP/IP, is also modeled in layers.

- The TCP/IP protocol stack consists of four layers: applications layer, transport layer, network layer, and data layer.

4.2 OSI and TCP/IP Model



4.2 OSI and TCP/IP Model

Application

- Applications communicate with each other over the network by using the data communication services of the transport layer.
- HTTP, file transfer protocol (FTP), SMTP, and SNMP telnet are some examples of the protocols working at the application layer.
- The data formatted at the application layer are called messages.

4.2 OSI and TCP/IP Model

Transport

- The transport layer provides end-to-end data transfer by delivering data from an application to its remote peer.
- Two main protocols work at the transport layer: the transmission control protocol (TCP) and the user datagram protocol (UDP).
  - TCP is referred to as a connection-oriented protocol because handshaking takes place before any data is sent.

4.2 OSI and TCP/IP Model

- UDP implements connectionless sessions via “best effort” delivery mechanisms.

Network

- The network layer is also called the *Internet layer or the Internetwork layer*.
- The transport layer needs to determine the routes between endpoints to transfer the end-to-end data, and the network layer provides the network routing services or IP addresses.

4.2 OSI and TCP/IP Model

- The protocol used to provide these services over the Internet is the Internet protocol (IP).

- ICMP, IGMP, ARP, and RARP are some examples of the protocols working at the network layer.

4.2 OSI and TCP/IP Model

- Data
  - The data layer is also called the network interface layer or the link layer.
  - The data layer is the interface to the actual network hardware.
  - IEEE 802.2, X.25 ATM, FDDI, SNA, PPP, Frame Relay, ATM, and IEEE 802.3 are some examples.
  - The data formatted at the data layer are called frames.

4.3 Sec. Pol., Serv., & Mech.

- Security Policies states an organization's intentions and decisions on what and how electronic information should be secured.

- The RFC 2828, "Internet Security Glossary" about security policy, security services, and security mechanisms.

4.3 Sec. Pol., Serv., & Mech.

- Security policy:
  - (1) A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.
  - (2) The set of rules laid down by the security authority governing the use and provision of security services and facilities.

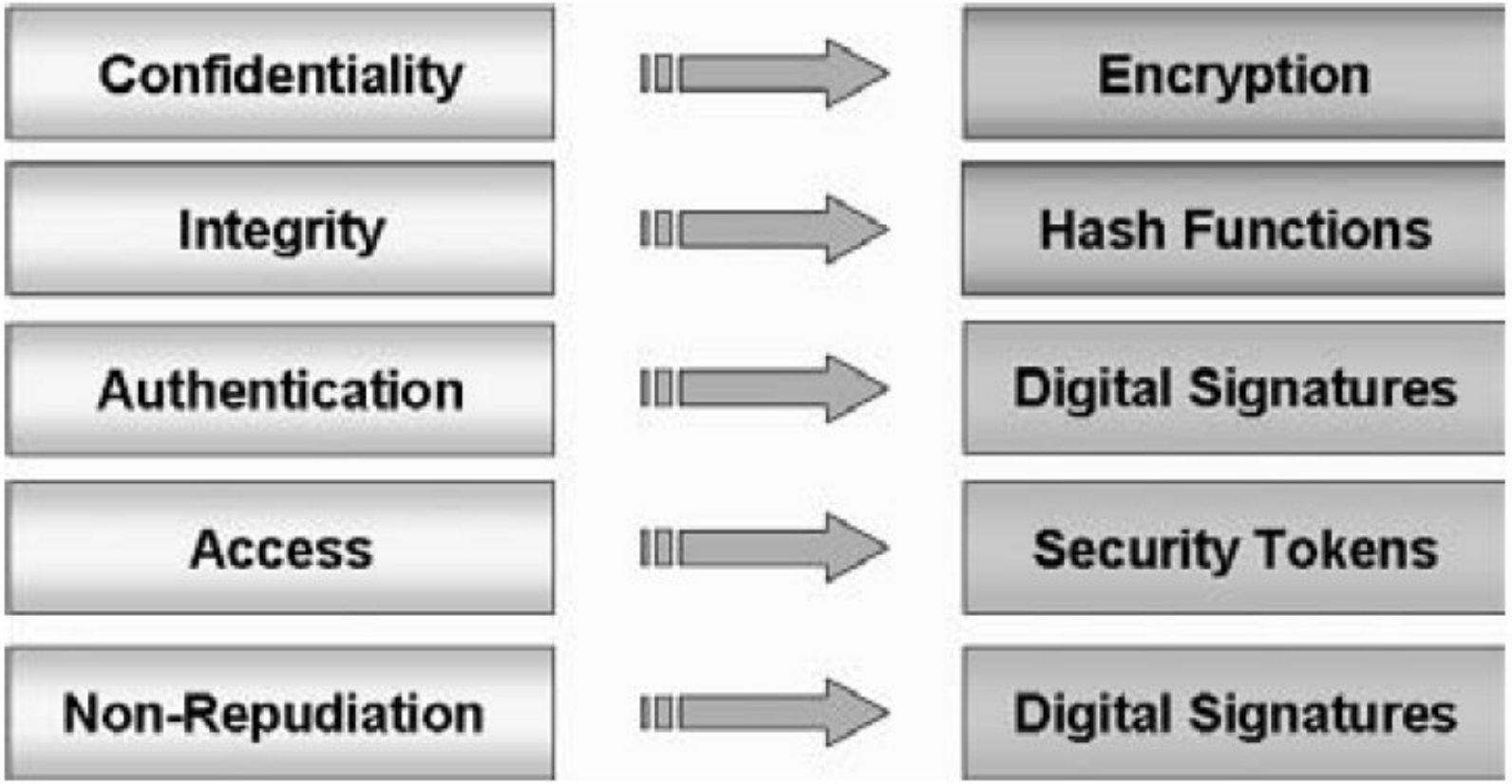
4.3 Sec. Pol., Serv., & Mech.

- Security devices:
  - A processing or communication service that is provided by a system to give a specific kind of protection to system resources.
- Security mechanisms:
  - A process (or a device incorporating such a process) that can be used in a system to implement a security service that is provided by or within the system.

4.3 Sec. Pol., Serv., & Mech.

Mechanism / Service	Encryption	Digital Signature	Access Control	Data Integrity	Authentication
Peer Entity Auth.	Y	Y			Y
Data Origin Auth.	Y	Y			
Access Control			Y		
Confidentiality	Y				
Traffic Flow Confidentiality	Y				
Data Integrity	Y	Y		Y	
Non-repudiation		Y		Y	
Availability				Y	Y

4.3 Sec. Pol., Serv., & Mech.

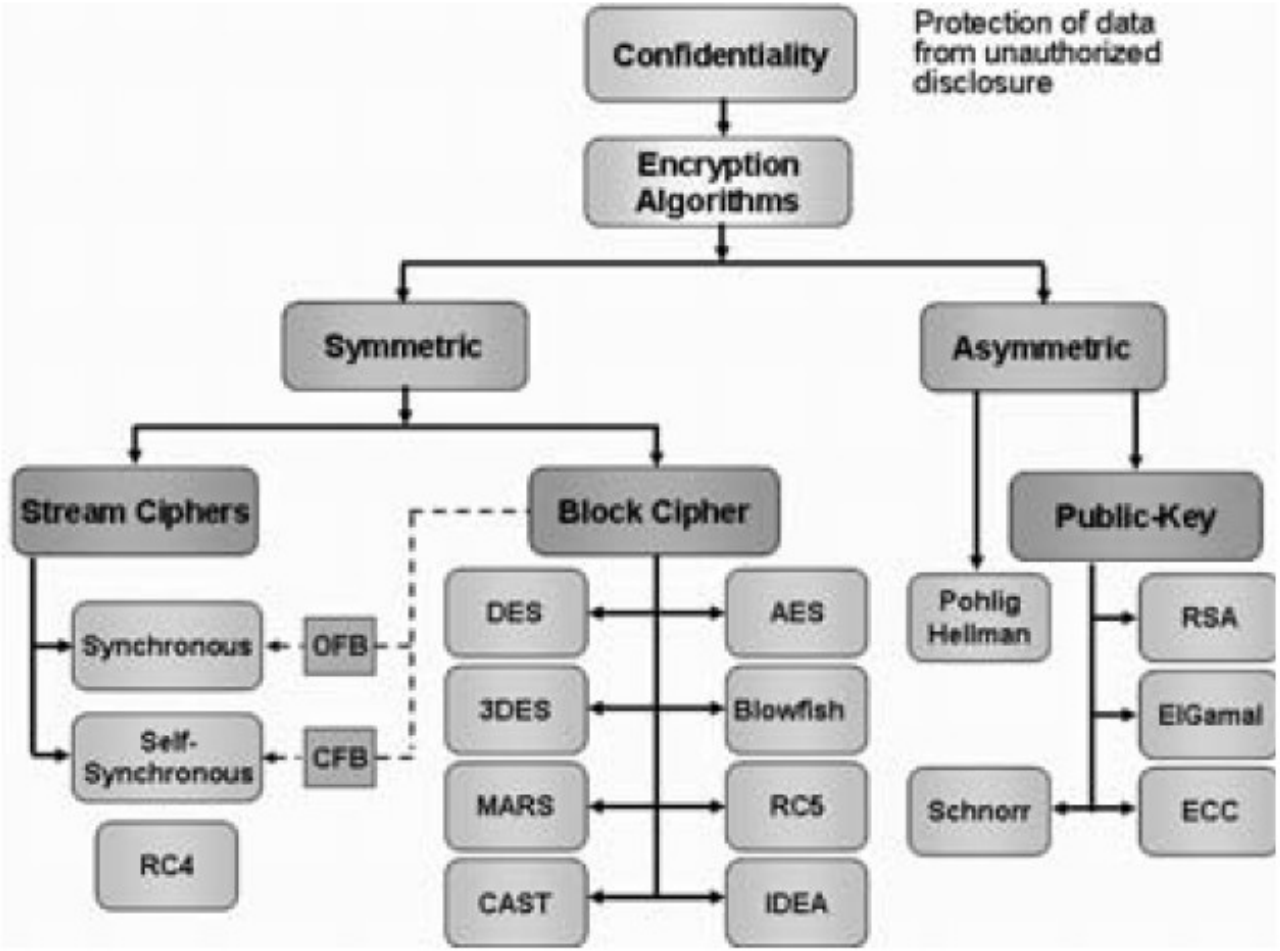


4.3 Sec. Pol., Serv., & Mech.

Confidentiality

- Confidentiality is the assurance that information is not made available or disclosed to unauthorized individuals, entities, or processes.

4.3 Sec. Pol., Serv., & Mech.

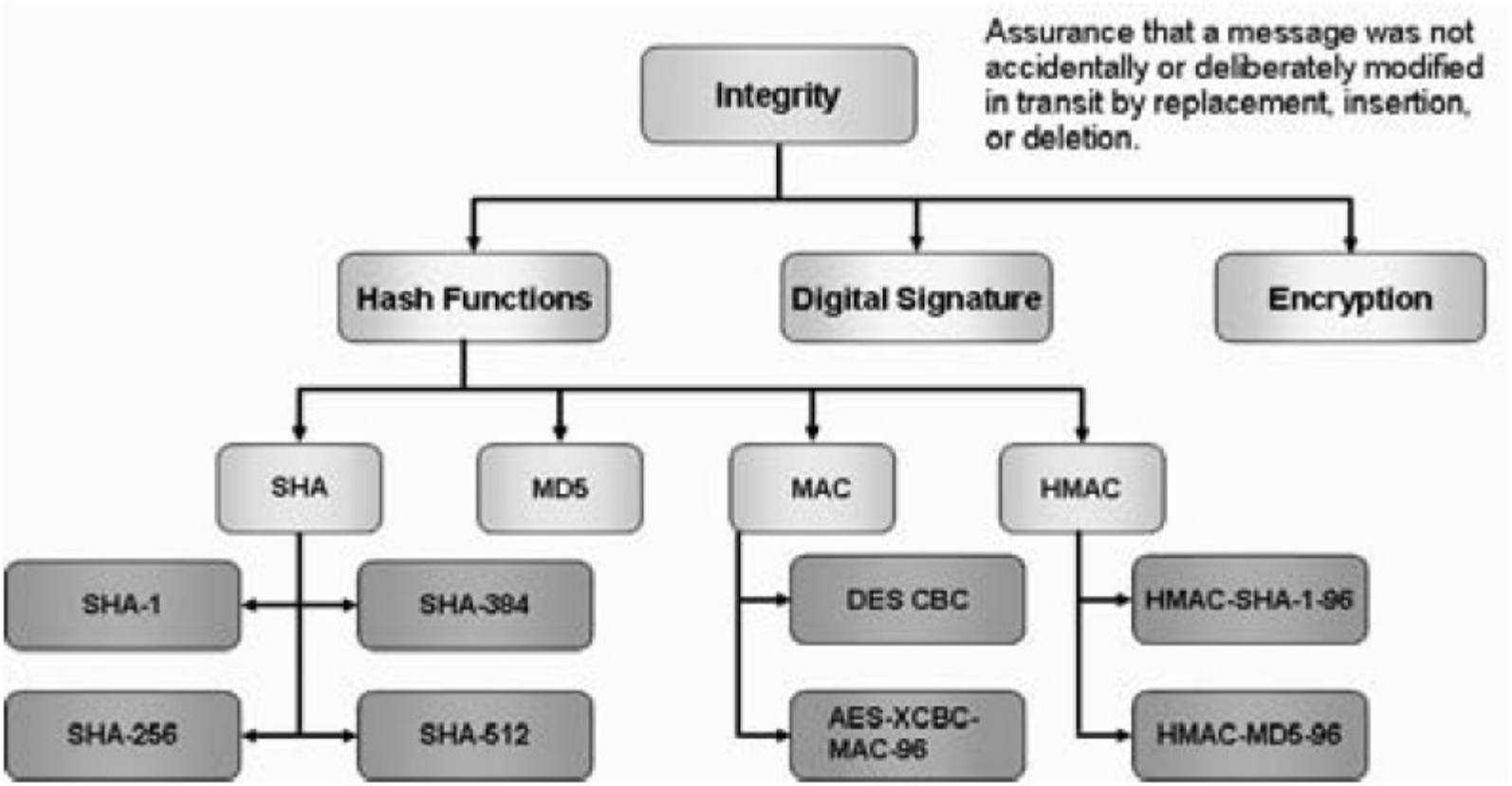


4.3 Sec. Pol., Serv., & Mech.

Integrity

- Integrity is the assurance that data is not accidentally or deliberately modified in transit by replacement, insertion, or deletion.

4.3 Sec. Pol., Serv., & Mech.

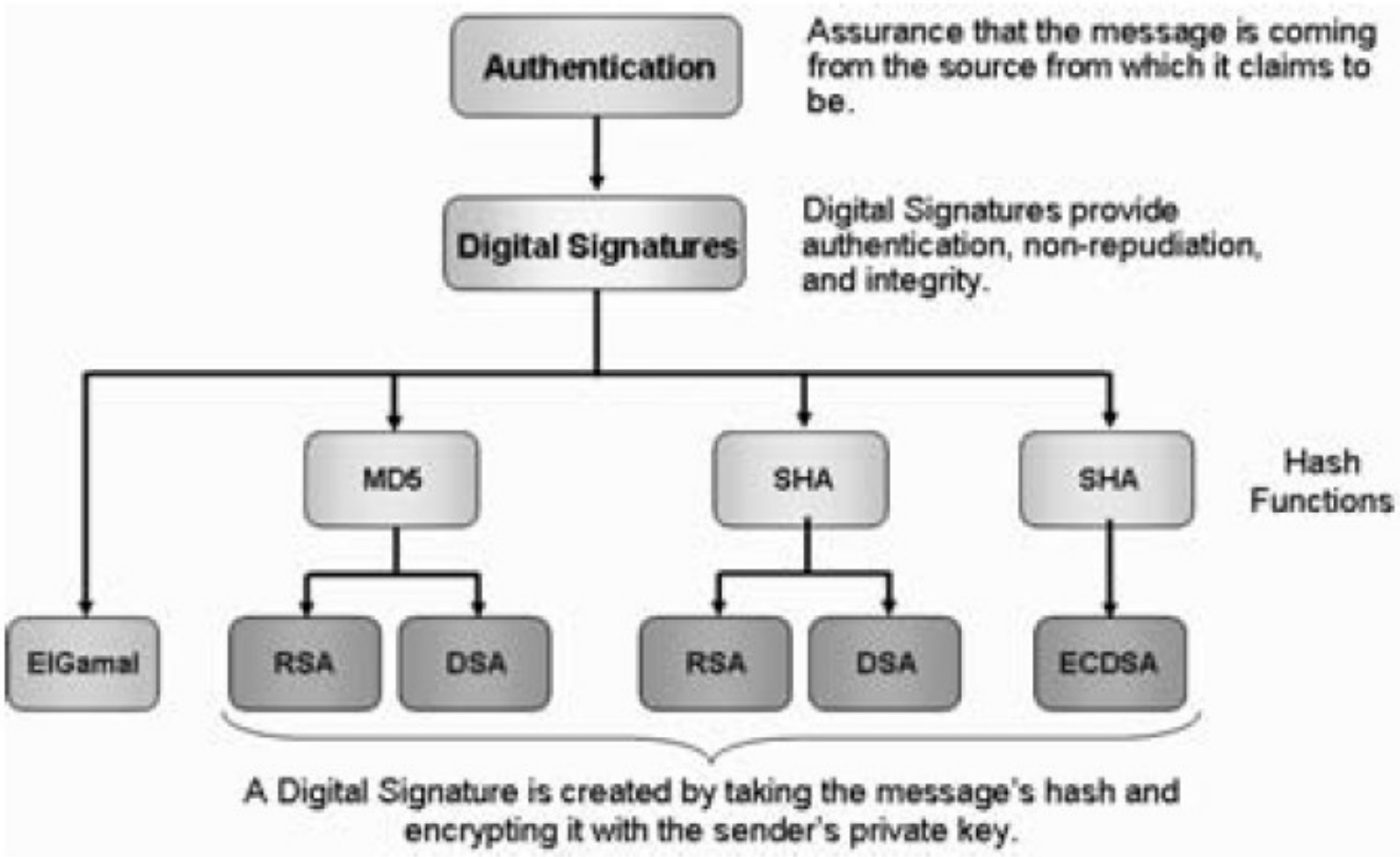


4.3 Sec. Pol., Serv., & Mech.

Authentication

- Authentication is the assurance that a message is coming from the source from which it claims to come.

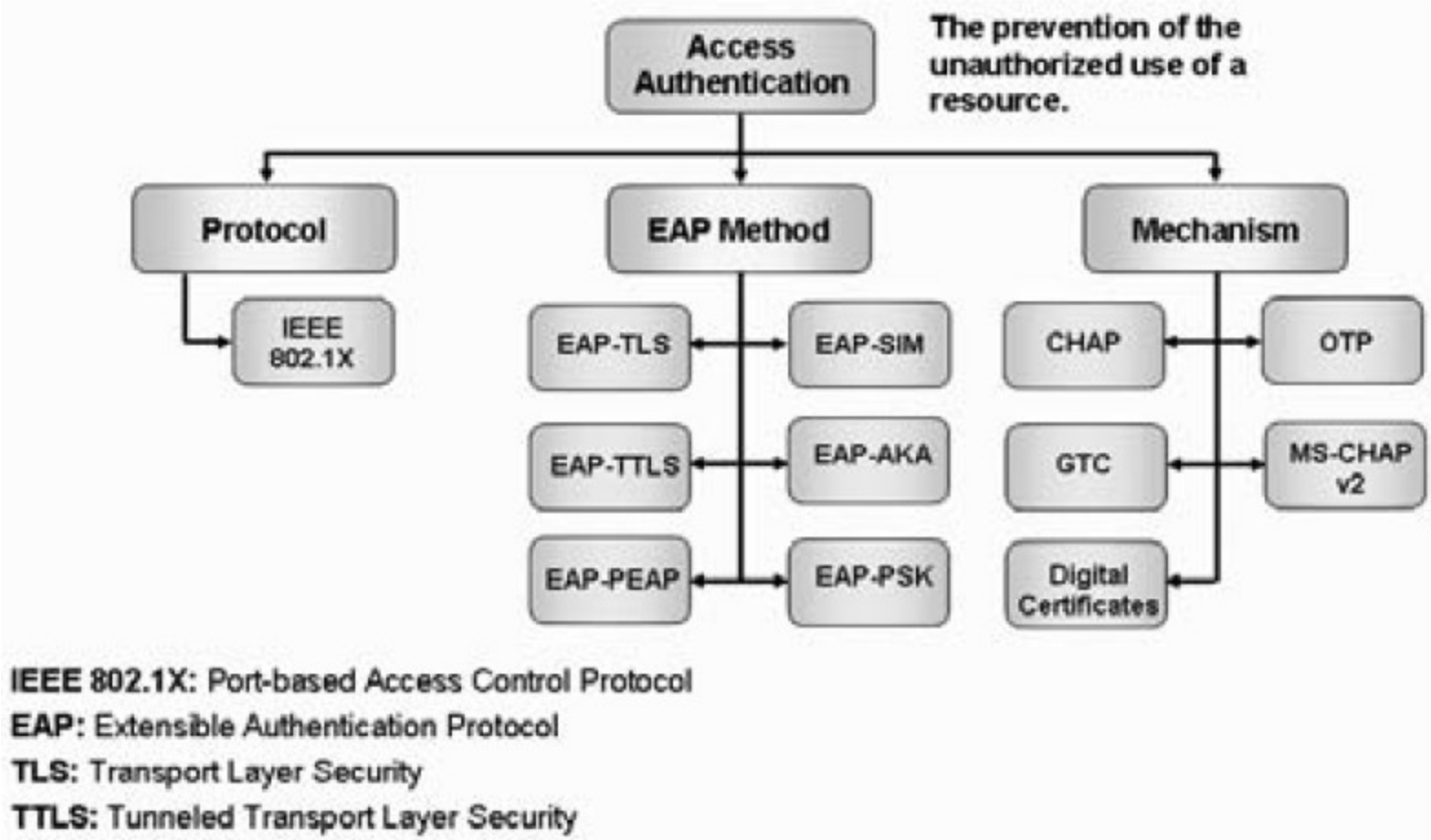
4.3 Sec. Pol., Serv., & Mech.



4.3 Sec. Pol., Serv., & Mech.

- *Access Control Authentication*
  - Access control provides protection against the unauthorized use of resources.
  - It includes the prevention of the use of a resource in an unauthorized manner by identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information.

4.3 Sec. Pol., Serv., & Mech.



4.3 Sec. Pol., Serv., & Mech.

- *Nonrepudiation*
  - Repudiation means denial by one of the entities involved in a communication of having participated in all or part of the communication.

4.3 Sec. Pol., Serv., & Mech.