Institute of Public Administration
Communication and Network Security
Group 1
Homework (2) Solution

Question (1)

Discuss in concisely the functionalities of OSI layers model.

Solution:

- The application layer serves as an interface between applications and network programs.
  It supports application programs and end-user processing.
  Common application-layer programs include remote logins, file transfer, email, and Web browsing.
- The presentation layer is responsible for dealing with data that is formed differently. This protocol layer allows application-layer programs residing on different sides of a communication channel with different platforms to understand each other's data formats regardless of how they are presented.
- The session layer is responsible for creating, managing, and closing a communication connection.
- The transport layer is responsible for providing reliable connections, such as packet
  Sequencing, traffic control, and congestion control.
- The network layer is responsible for routing device-independent data packets from the current hop to the next hop.
- The data-link layer is responsible for encapsulating device-independent data packets into device-dependent data frames.
  It has two sublayers: logical link control and media access control.
- The physical layer is responsible for transmitting device-dependent frames through some physical media.

Question (2)
What are the functions of PKIs setup?

Solution:

1. Determine the legitimacy of users before issuing public-key certificates to them.
2. Issue public-key certificates upon user requests.
3. Extend public-key certificates valid time upon user requests.
4. Revoke public-key certificates upon users' requests or when the corresponding private keys are compromised.
5. Store and manage public-key certificates.
6. Prevent digital signature signers from denying their signatures.
7. Support CA networks to allow different CAs to authenticate public-key certificates issued by other CAs.

Question (3)
What is the purpose from using IPsec protocol?

Solution:
IPsec provides a potent platform for constructing virtual private networks (VPN), and VPNs are private networks overlayed on public networks.

Question (4)
What are the components of SSL protocol?

Solution:
SSL consists of two components:
The first component is referred to as the record protocol, which is placed on top of transport-layer protocols.
The second component consists of the handshake protocol, the change-cipher-spec protocol, and the alert protocol.

Question (5)
Discuss the purpose of MIME protocol.

Solution:
The Multipurpose Internet Mail Extension protocol (MIME) was designed to support sending and receiving email messages in various formats, including nontext files generated by word processors, graphics files, sound files, and video clips. Moreover, MIME allows a single message to include mixed types of data in any combination of these formats.

Question (6)

Discuss the purpose of Kerberos protocol?

Solution:

The purpose of Kerberos is to make it easy for users to authenticate themselves to various servers at the local network (e.g., email server, Web server, and file server) for obtaining services, without needing to type in their passwords every time before they use the service.

Question (7)

Discuss and describe the layers of SSH protocol.

Solution:

The SSH divided into three layers as following:

- Connection layer.
- The user authentication layer.
- The transport layer.

The SSH transport layer is the bottom layer. It is used to authenticate server, exchange keys in the initial phase, and set up encryption and compression algorithms.

The user's computer ensures that it is connecting to the same server computer during subsequent sessions.

Subsequent packets transmitted between the client and the server are all encrypted using a symmetric-key encryption algorithm.

Question (8)

Name one electronic voting protocol?

Solution:

The Helios Voting Protocol