FIT3031 Tutorial 1 Sample Solution

INTRODUCTION TO INFORMATION & NETWORK SECURITY

Review Questions

1. What are the three issues OSI security architecture focuses on?

Ans: OSI Security Architecture focuses on three aspects of information security : security attacks, security mechanisms, security services

2. What are the differences between passive attack and active attack?

Ans: Passive attack has the nature of eavesdropping on, or monitoring of, transmission of information between the communicating parties, but does not modify of temper the message. It captures the message and may read the content. It can be used for traffic analysis e.g., who is a particular person communicating with and the frequency of communication.

Active attack modifies a message stream or creates a false message. It is used to launch more severe form of attack.

3. Describe different types of passive attacks.
Ans: Two types:

Release of message content: captures and read the content.

Traffic analysis: does not read the message but observes the pattern. Observation usually involves determining the location and identity of communicating parties, frequency and length of communication.

4. Describe different types of active attacks.
Ans: Four types:

Masquerade: assumes a false identity.

Replay: passive capture of data and subsequent retransmission

Modification of Message: message is altered, delayed or reordered to produce unauthorized effect

Denial of Service: cripple the server with a flood of requests; eat up all the computing resources of the server, causes disruption of services of an entire network or suppression of all messages directed to a particular destination.

5. What are the six main security services defined by OSI security architecture? Briefly describe each of them.

Ans: They are the followings:

Confidentiality - protects data from unauthorized discloser.
Authentication - assures that the communication is authentic; communicating entities are who they claim to be.
Integrity - no alteration of data.
Non-repudiation - prevents sender or receiver from denying transmitting or receiving a message.
Access control - limits and controls access to the host systems and applications; only the legitimate users are allowed to use certain application on the host system.
Availability - assures that the service is available to legitimate users.

6. Name six security mechanisms.

Ans: They can be one of those list in lecture slide#31, e.g., encipherment, digital signatures, access controls, data integrity, authentication exchange, security audit trails etc.

7. Describe the model for network security as shown in Figure 1.4 below. What are the components it should have? What are the basic tasks that such a model should perform?

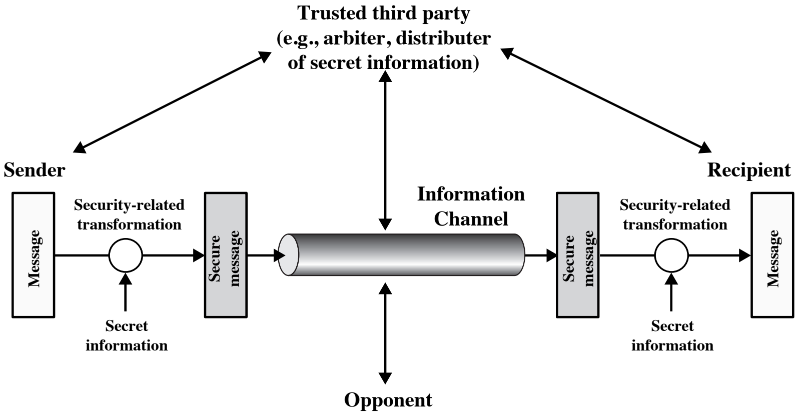

Figure 1.4 Model for Network Security

Ans: The model in Figure 1.4 has a few components: sender (originating a message), encryption algorithm, secret key, decryption algorithm and the recipient (receiving the message). This model requires the following tasks to be done.

i. design a suitable algorithm for the security transformation
ii. generate the secret information (keys) used by the algorithm
iii. develop methods to distribute and share the secret information
iv. specify a protocol enabling the principals to use the transformation and secret information for a security service

Problems

1. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

Ans: The system must keep personal identification numbers confidential, both in the host system and during transmission for a transaction. It must protect the integrity of account records and of individual transactions. Availability of the host system is important to the economic well being of the bank, but not to its fiduciary responsibility. The availability of individual teller machines is of less concern.

2. Consider a desktop publishing system used to produce documents for various organizations.
    a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
    Ans: The system will have to assure confidentiality if it is being used to publish corporate proprietary material.

    b. Give an example of a type of publication for which data integrity is the most important requirement.
    Ans: The system will have to assure integrity if it is being used for laws or regulations.

    c. Give an example in which system availability is the most important requirement.
    Ans: The system will have to assure availability if it is being used to publish a daily newspaper.

3. Consider a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller. Give examples of confidentiality, integrity and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.

Ans:

- The system does not have high requirements for integrity on individual transactions, as lasting damage will not be incurred by occasionally losing a call or billing record.
- The integrity of control programs and configuration records, however, is critical. Without these, the switching function would be defeated and
- the most important attribute of all - availability - would be compromised. A telephone switching system must also preserve the confidentiality of individual calls, preventing one caller from overhearing another.

4. For each of the following assets, assign a low, moderate or high impact level for the loss of confidentiality, availability and integrity, respectively. Justify your answers.
    a. An organization managing public information on its Web server.
    Ans: An organization managing public information on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability.

    b. A law enforcement organization managing extremely sensitive investigative information.
    Ans: A law enforcement organization managing extremely sensitive investigative information determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate.

    c. A financial organization managing routine administrative information (not privacy-related information).
    Ans: A financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low.

    d. An information system used for large acquisitions in a contracting organization that contains both sensitive pre-solicitation phase contract information and routine administrative information. Assess the impact of the 2 datasets separately and the information system as a whole.
    Ans: The management within the contracting organization determines that:
    (i) for the sensitive contract information,
        - the potential impact from a loss of confidentiality is moderate,
        - the potential impact from a loss of integrity is moderate, and
        - the potential impact from a loss of availability is low; and

    (ii) for the routine administrative information (non-privacy-related information),

- the potential impact from a loss of confidentiality is low,
- the potential impact from a loss of integrity is low, and
- the potential impact from a loss of availability is low.

e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact of the 2 datasets separately and the information system as a whole.
Ans: The management at the power plant determines that:
   (i) for the sensor data being acquired by the SCADA system,
      - there is no potential impact from a loss of confidentiality,
      - a high potential impact from a loss of integrity,
      - and a high potential impact from a loss of availability; and
   (ii) for the administrative information being processed by the system,
      - there is a low potential impact from a loss of confidentiality,
      - a low potential impact from a loss of integrity, and
      - a low potential impact from a loss of availability.