FIT2093: Tutorial 1 Sample Solutions

Introduction to cyber security

Review Questions

1. What is cyber security?

   Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

2. Distinguish or define the terms within the context of security: Vulnerability, Threat and Control.

   Vulnerability is a weakness in a security system, that might be exploited to cause loss or harm. It is a means by which a threat agent can cause harm. A threat is a set of circumstances that has the potential to cause loss or harm. A control is a protective measure that prevents a threat agent from exercising vulnerability. That is, a control is an action, device, procedure, or technique that removes or reduces vulnerability.

3. Categorise the type of security threats (or attacks) to computers/distributed systems/computer networks (also known as logical security risks).

   a. Interruption: attack on availability
   b. Interception: attack on confidentiality
   c. Modification: attack on integrity
   d. Fabrication: attack on authenticity

4. Give an example to each of the above category – can be your own personal computer, corporate computer systems such as Monash University, etc. Relate those threats to hardware/software/data as applied to corporate computer systems.

   The answers can vary: There are some answers outside the scope of this subject! This can be answered using examples as follows:

   i. Interruption: send a huge numbers of **icmp** packets using ping command from thousands of machine to one specific computer to increase processing load so eventually the machine cannot provide any other services.
   ii. Interception: using packet sniffer software to detect data transmitted across the network even the data is transmitted in cipher text in attempt to retrieve plaintext. The main purpose of this kind of attack is to retrieve cryptographic keys.

iii. Modification: an attacker intercepts a message; changes its content, and sends to intended recipient. The recipient receives the message without being aware that the content of the message has been changed.
iv. Fabrication: initially, an attacker needs to have a secret key shared between Alice and Bob. The attacker applies a cryptographic operation with the key to a message and sends it to the Bob. Bob receives the message without being aware that the message has not been sent from Alice.

Note that, to succeed in modification and fabrication, the attacker needs to have the cryptographic key, which can be retrieved by interception.

5. Enumerate the desirable security properties for overall security?

    i. Confidentiality (Privacy is an aspect of confidentiality related to personal information of individuals): assures prevention of unauthorised disclosure of information
    ii. Availability: System works promptly and service is not denied to authorised users
    iii. Integrity: Assures information modification by authorised personnel only

    Others are

    iv. Non-repudiation: Sender/receiver cannot deny having sent/received information
    v. Authenticity: undisputed origin/genuine
    vi. Accountability: responsible for actions
    vii. Reliability: trustworthiness

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

    Passive attack has the nature of eavesdropping on, or monitoring of, transmission of information between the communicating parties, but does not modify or tamper 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 forms of attack.

7. Describe different types of passive attacks and active attacks.

    a. Passive attacks, 2 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.

b. Active attacks, 4 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.

8. List and briefly define categories of security services.

   Authentication: The assurance that the communicating entity is the one that it claims to be.

   Access control: The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

   Data confidentiality: The protection of data from unauthorized disclosure.

   Data integrity: The assurance that data received are exactly as sent by an
   authorized entity (i.e., contain no modification, insertion, deletion, or replay).

   Nonrepudiation: Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

   Availability service: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

9. List and briefly define categories of security mechanism.

SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of
the OSI security services.

i. **Encipherment**
   The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
ii. **Digital Signature**

Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

iii. **Access Control**
A variety of mechanisms that enforce access rights to resources.

iv. **Data Integrity**
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

v. **Authentication Exchange**
A mechanism intended to ensure the identity of an entity by means of information exchange.

vi. **Traffic Padding**
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

vii. **Routing Control**
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

viii. **Notarization**
The use of a trusted third party to assure certain properties of a data exchange.

Problems

1. Preserving confidentiality, integrity, and availability of data is a restatement of the concern over interruption, interception, modification, and fabrication. How do the first three concepts relate to the fourth one? That is, is any of the four equivalent to one or more of the three?

   There is no one-to-one correspondence. Modification is primarily a failure of integrity, although there are aspects of availability (denial of service). Fabrication is probably the closest to being exclusively an integrity violation, although fabrication of covert outputs could be used to leak otherwise confidential data. Interruption is an availability concern although one can argue that is also a failure of integrity of a communication or information flow. Interception primarily results in a breach of confidentiality, although it could also be seen as an attack on availability.

2. It is stated that it is impossible to design security mechanism(s) to shield any kind of security attacks - Why is this statement true?

   a. Yes. Even the so-called very secure security mechanism suffers from human errors which can be given as follows:

i. Error during design phase. The design error may not yet be discovered right after the mechanism has been implemented and may not affect the functionality of the mechanism. However, it may offer the possibility to attacks if an attack can make use of some of its errors.
ii. Error during implementation phases. As most of the security mechanisms deploy cryptographic operations, which rely on secret keys. The misbehaviour of users regarding storing and using secret keys may compromise the security of the system.

3. One control against accidental software deletion is to save all old versions of a program. Of course, this control is prohibitively expensive in terms of cost of storage. Suggest a less costly control against accidental software deletion. Is your control effective against all possible causes of software deletion? If not, what threats does it not cover?

   Save incremental copies: only the changes since the last change. Equivalently save a "transaction journal" of changes since last full back-up. Develop a configuration management approach to save code necessary to create a new version from the old.

4. For a user workstation in a typical business environment, list potential locations for confidentiality attacks.
   a. LAN.
   b. Dial-in communications server.
   c. Internet
   d. Wiring closet

5. You discover that your computer has been infected by a piece of malicious (virus) code. You have no idea when the infection has occurred. You do have backups performed every week since the system was bought, but, offcourse, there have been numerous changes to the system over time. How could you use the backups to construct a "clean" version of your computer system?

   Impossible way: Start from the beginning and rebuild from first backup, applying all changed in order.
   Potentially feasible way: Compare files of original backup with current files. Try to account for differences (new files, changed file sizes). Review all backup to determine when each file was changed or created. Note this is also a difficult task.

6. 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.

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.

7. 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.
    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.
    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.
    The system will have to assure availability if it is being used to publish a daily newspaper.