UBUA VERA

16/SCI01/048

COMPUTER SCIENCE

400 LEVEL

CSC 418: COMPUTER SECURITY REVISED QUESTIONS 2019/2020

1. Computer and network systems have given us unlimited opportunities to reduce costs, improve efficiency, and increase revenues. Unfortunately, our dependence on computer and network systems has also exposed us to new risks which threaten the security of computer and network systems and present new challenges for protecting our assets and information on computer and network systems. Justify.

2. Describe the level of security impact in relation to confidentiality, integrity and availability on the following scenario: i. Student enrolment information ii. Anonymous online poll. iii. Public Web site for a university.

3. Differentiate between data integrity and system integrity.

4. Computer and network security is both fascinating and complex, justify.

5. Define the following: i. Security Attack ii. Security Mechanism iii. Security services.

6. What is computer security? Using relevant examples, describe four key objectives of computer security.

7. Security attack is classified into two. State and define them.

8. What is the goal of a passive attack and active attack?

9. There are two types of Passive attack, discuss with a given example or scenario.

10. What is the only means that is feasible to prevent the success of passive attacks?

11. Active attack is classified into four categories, list and discuss using a given example or scenario.

12. Define Security service as discuss by I. X800 and ii. RFC 4949.

13. Define the following: I. Authentication ii. Peer entity authentication iii. Data – origin authentication IV. Access Control v. Data confidentiality VI. Data integrity vii. Non Repudiation

14. Highlights and define four types of confidentiality.

ANSWERS

1. Computer security is also a concern of individuals, including many who neither use nor possess computer systems. If data can be accessed improperly, or if systems lack adequate safeguards, harm may come not only to the owner of the data, but also to those to whom the data refers. The volume and nature of computerized data-bases mean that most of us run the risk of having our privacy violated in serious ways. This is particularly worrisome, since those in a position to protect our privacy may have little incentive to do so
2. NNCCBSCBJHJ
3. Differences between data integrity and system integrity

|  |  |
| --- | --- |
| DATA INTEGRITY | SYSTEM INTEGRITY |
| * Data integrity is when the data in memory or stored is Inna state that in make sense from a functional perspective. You reach data integrity by using data management systems that supports ACID principles and when you have coherent data model. | * System integrity includes all elements of a system, which is likely to contain several information system components, including a database. |
| * Assures that information and programs are changed only in a specified and authorized manner. | * Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. |
| * **Refers to the overall accuracy, completeness, and consistency of data. Data integrity also refers to the safety of data in regards to regulatory compliance and security** | * Refers to the capability of performing correctly according to the original specification of the **system** under various adversarial conditions. |

1. Computer and network security is both fascinating and complex, justification:

a. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

b. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.

c. Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.

d. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.

e. security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed.

5. Security Attack: An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.

ii. Security Mechanism:  are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service.

iii. Security services: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

1. What is computer security? Using relevant examples, describe four key objectives of computer security

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

Objective of computer security

* Confidentiality: keeping information away from people who should not have it. Accomplishing this objective requires that we know what data we are protecting and who should have access to it. It requires that we provide protection mechanisms for the data while it is stored in the computer and while it is being transferred over networks between computers.
* Integrity: assuring that the information stored in the computer is never contaminated or changed in a way that is not appropriate. Both confidentiality and availability contribute to integrity.
* Availability: ensuring that data stored in the computer can be accessed by the people who should access it. Availability is a broad subject addressing things such as fault tolerance to protect against denial of service and access control to ensure that data is available to those authorized to access it. Most computers can at least differentiate between two classes of users: system administrators and general end users.
* Non-repudiation: This principle does not allow the sender or a message to refute the claim of not sending that message. It provides protection against denies by one of the entities involved in a

1. Classification of security attacks

* Passive Attack: Passive attacks are those, where the attacker aims to obtain the information. They do not wish to modify the content of original message. It is very difficult to detect as it does not alter the data. Releases of message, traffic analysis, sniffing and key loggers are some techniques of passive attacks.
* Active Attack: Active attacks are attacks which make some modification in the original message or creation of some false message. These attacks are very complex and cannot prevent easily. It can further categorize into 3 types: Interruption, Fabrication, and Modification. Under these categorize Denial of service (DoS), DDoS, DRDoS, SQL Injection, Replay attack, Masquerading,

Man in Middle Attacks are some common attacks.

1. The goal of passive attack:
2. Types of passive attack:

* **The release of message content –**  
  Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.
* **Traffic analysis –**  
  Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.  
  The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

1. . What is the only means that is feasible to prevent the success of passive attacks?

It is feasible to prevent the success of these attacks, usually by means of encryption.

1. Classification of active attacks includes:

* **Masquerade –**  
  Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.
* **Modification of messages –**  
  It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.
* **Replay –**  
  It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.
* **Denial of Service –**  
  It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.

1. Security service as discuss by I. X800 and ii. RFC 4949.

* RFC 4949: it is a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.
* X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

1. Define the following:

* Authentication: Authentication ensures that entities do communication is the correct entity. This service is ensure there is no interference from the third of the communication is done.
* Peer entity authentication: Peer entity authentication provide evidence the identity of the connected entities. It is used at the time of formation and during transfer the data from a connection.
* Data – origin authentication: Data origin authentication provides evidence source of the data unit. Provide assurance that the source of the data is claimed.
* Access Control: The ability to limit and control access to the host system and applications use an communication. Its implementation is done by early identification of the entity that will enter the lines of communication. Prevent users not authorized to access the resource.
* Data confidentiality: Trasmisi protect data from passive attacks and ensure no changes to the data attack. The aspects that exist in Data confidentiality.
* Data integrity: Data integrity is the assurance that the data received is really from the data sent from the correct sender. That is not changes occur during data transmission performed.
* Non Repudiation: Prevent sending or receiving deny that the message is correct messages been sent / received.

1. Types of confidentiality

* **Connection Confidentiality:** The protection of all user data on a connection.
* **Connectionless Confidentiality:** The protection of all user data in a single data block
* **Selective-Field Confidentiality:** The confidentiality of selected fields within the user data on a connection or in a single data block.
* **Traffic-Flow Confidentiality:** The protection of the information that might be derived from observation of traffic flows.