**NAME: DABO LAURA I.**

**MATRIC NUMBER: 16/SCI01/053.**

**COURSE CODE: CSC 418.**

**COURSE TITLE: INFORMATION SYSTEMS SECURITY.**

**ASSIGNMENT TITLE: REVISED QUESTIONS PART A.**

**Kindly use these questions to revise the topics we have treated so far. It will come in batches, this is the first batch. The rest will be posted as times goes on.**

**Kindly attempt it and submit online.**

**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:
3. Student enrollment information
4. Anonymous online poll.
5. Public Web site for a university.
6. Differentiate between data integrity and system integrity.
7. Computer and network security is both fascinating and complex, justify.
8. Define the following:
9. Security Attack
10. Security Mechanism
11. Security Services.
12. What is computer security? Using relevant examples, describe four key objectives of computer security.
13. Security attack is classified into two. State and define them.
14. What is the goal of a passive attack and active attack?
15. There are two types of Passive attack, discuss with a given example or scenario.
16. What is the only means that is feasible to prevent the success of passive attacks?
17. Active attack is classified into four categories, list and discuss using a given example or scenario
18. Define Security service as discuss by
19. X800 and
20. RFC 4949.
21. Define the following:
22. Authentication
23. Peer entity authentication
24. Data origin authentication
25. Access Control
26. Data confidentiality
27. Data integrity
28. Non Repudiation
29. Highlights and define four types of confidentiality.

**ANSWERS**

1. It has exposed us to system vulnerabilities and threats to our assets and transactions on those systems. The protection of computer and network security must cover prevention to reduce system vulnerabilities, detection to identify on-going cyber-attacks that break through prevention mechanisms and response to stop and control cyber-attacks, recover systems and correct exploited system vulnerabilities.

Computer and network security is concerned with availability, confidentiality, integrity, non-repudiation, trust, and many other aspects of computer and network assets which may be compromised by cyber-attacks from external and insider threats through exploiting system vulnerabilities. For example, Nathan transmits a file to Jemima. The file contains sensitive information that is to be protected from disclosure. Peace, who is not authorized to read the file is able to monitor the transmission and capture a copy of the file during its transmission.

1. Student enrolment information

Moderate confidentiality: this information is seen by more people on a daily basis, is less likely to be targeted than grade information, and results in less damage if disclosed.

1. Anonymous online poll.

Low integrity: Many Web sites, such as news organizations, offer these polls to their users with very few safeguards. However, the inaccuracy and unscientific nature of such polls is well understood.

1. Public Web site for a university.

Moderate availability: the Web site provides information for current and prospective students and donors. Such a site is not a critical component of the university’s information system, but its unavailability will cause some embarrassment.

1. Data integrity is the word that deals with the maintenance and consistency of data. It assures that information and programs are changed only in a specified and authorized manner. For example, you have two database tables with some column names and to retrieve the data from two tables, we need integrate them into one single database table. Whereas, system integrity deals with the state of system and its performance, independent of its platform and undisturbed by its outside or inside changes. In easy words, system integration can be defined as the consistent working of a system independent of its input functions and external environments. It assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
2. Computer and network security is both fascinating and complex with the following reasons;
3. Security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather delicate reasoning.
4. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
5. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense (e.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed).
6. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behaviour may complicate the task of developing the security mechanism.
7. Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.
8. 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.
9. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.
10. Security attack can be defined as any action that compromises the security of information owned by an organization.
11. Security mechanism can be defined as a process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
12. Security services can be defined as a processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.
13. Computer security is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources. It is basically the protection of computer systems and information from harm, theft and unauthorized use.
14. Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information. This term covers two related concepts which are data confidentiality (assures that private or confidential information is not made available or disclosed to unauthorized individuals) and privacy (assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed). For example, Rachael wants to send a message to Amina. She will either put a password or change the message to an encoded form so that anyone without authorization can read it.
15. Integrity is guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

This term covers two related concepts which are data integrity (assures that information and programs are changed only in a specified and authorized manner) and system integrity (assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system). For example, a company with sensitive data. Only the administration users will be given privileges to alter or modify the data of the company.

1. Availability deals with ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system. For example, a school is conducting online examination. The ICT department have to ensure that all students get access to their questions and the questions have to conform with their irrespective courses.
2. Non repudiation ensures protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. It prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message. For example, Bob sends a message to Alice but before sending it he encrypts the message. When Alice receives the encrypted message, she has to decrypt the message which can only be done through the use of signature. The signature is like a password.
3. Security Attack are classified into two namely; passive attack and active attack
4. Passive attack can be defined as attempts to learn or make use of information from the system but does not affect system resources. They are in the nature of eavesdropping on or monitoring of transmission.
5. An active attack can be defined as attempts to alter system resources or affect their operation. It involves some modification of the data stream or creation of false statement.
6. In a passive attack, the goal of the opponent is to obtain information that is being transmitted. Whereas in an active attack, the goal is to detect active attacks and to recover from any disruption or delays caused by them. If the detection has a deterrent effect, it may also contribute to prevention.
7. Two types of passive attacks are the release of message contents and traffic analysis.
8. The release of message contents is easily understood. For example, A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. There must be a prevention of an opponent from learning the contents of these transmissions. For instance, the sender, Adriel will send a message to the receiver, David. A third party, Calm who is unauthorised will gain an access of the data without making any modification.
9. Traffic analysis, is subtler. Suppose there is a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. For instance, the sender, Adriel will send a message to the receiver, David. A third party, Calm who is unauthorised observes the traffic flow and based on this observable Calm will gain access to the data.
10. The only means that is feasible to prevent the success of passive attacks is usually by means of encryption.
11. Active attack is classified into four categories which are masquerade, replay, modification and denial of service
12. A masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges. For instance, a masquerade attacker, Knox gains access to the account of a legitimate user either by stealing the victim’s account ID and password and sends a message to the receiver, David.
13. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. For example, the sender, Adriel will send a message to the receiver, David and the third party, Calm who is not unauthorised gains access to the same message being sent by Adriel. Calm will modify the message and send it to David. David will receive the message twice (one from the sender and one from the unauthorised person) and he will not know which is from the authorised sender.
14. Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect. For example, a message meaning “Allow Chris to read confidential file X” is modified as “Allow Knox to read confidential file X”. Another example, Knox wants to send a message to Jenom but the message goes to Bambai who modifies the message and sends it to Jenom.
15. The denial of service prevents the normal use or management of communications facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). Another form of service denial is the disruption of an entire network withers by disabling the network or by overloading it by messages so as to degrade performance. For example, Mary who is unauthorised interrupts the services which are sent by the server to the sender in the name of the sender.
16. X800 defined 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.
17. RFC 4949 defined security service as 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.

1. Authentication can be defined as ensuring that the communicating entity is the one that it claims to be.
2. Peer entity authentication used in association with a logical connection to provide confidence in the identity of the entities connected.
3. Data origin authentication provides assurance that the source of received data is as claimed in a connectionless transfer.
4. Access control is the prevention of unauthorized use of a resource. It is the ability to limit and control the access to host systems and applications via communications links.
5. Data confidentiality assures that private or confidential information is not made available or disclosed to unauthorized individuals.
6. Data integrity assures that information and programs are changed only in a specified and authorized manner (i.e., contain no modification, insertion, deletion, or replay).
7. Non repudiation provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
8. The four types of confidentiality are;
9. Connection Confidentiality
10. Connectionless Confidentiality
11. Selective-Field Confidentiality
12. Traffic-Flow Confidentiality
13. Connection confidentiality can be defined as the protection of all user data on a connection.
14. Connectionless confidentiality can be defined as the protection of all user data in a single data block.
15. Selective-field confidentiality can be defined as the confidentiality of selected fields within the user data on a connection or in a single data block.
16. Traffic-flow confidentiality can be defined as the protection of the information that might be derived from observation of traffic flows.