**ADEYEMI TESLIMATADEBUNMI**

**16/SCI01/003**

**CSC418 ASSIGNMENT**

1.
2. Student Enrollment

Confidentiality- High

Integrity –High

Availability – High

Anonymous online poll

Confidentiality- High

Integrity –moderate

Availability – High

Public Website for university

Confidentiality- moderate

Integrity –moderate

Availability – High

1. Data integrity assures that information and programs change only in a specified and authorized manner, while system integrity assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

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. While System integrity includes all elements of a system, which is likely to contain several information system components, including a database.

1. 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, and integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning. 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.
2. A security attack is an unauthorized attempt to steal, damage, or expose data from an information system such as your website.

Security Mechanism are techniques used to implement the authentication and authorization, e.g., credentials, capacities, cryptographic transformations such as signature and encryption, access control lists (ACL).

Security services is the 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.

1. 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 (such as hardware, software, firmware, information/data, and telecommunications). Computer Security is also the protection of computer systems and information from harm, theft, and unauthorized use.

Confidentiality: this is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. For example; Medical information is an asset whose confidentiality is considered to be highly important by patients. Medical information should only be available to the patient, their parents, and employees that require the information to do their job.

Integrity: this is guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. For example; Patient allergy information is an example of an asset with a high requirement for integrity. The doctor should be able to trust that the information is correct and current.

Availability: this deal 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;

1. Passive Attack

Active Attack

* Passive Attack is attempts to learn or make use of information from the system but does not affect system resources.
* Active attack attempts to alter system resources or affect their operation.
1. The goal of passive attack is to obtain information that is being transmitted

The goal of Passive attack is to alter computer networks and systems resources or alter their operations.

1. 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. The only means feasible is usually by means of encryption.
2. *Masquerade*

 *replay,*

 *modification of messages,*

and *denial of service*.

* 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.
* Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. (paths 1, 2, and 3 active)
* 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. (paths 1 and 2 active)
* The denial of service prevents or inhibits the normal use or management of communications facilities (path 3 active). 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).
1. X800- X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.

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.

1. Authentication- It is the process of recognizing a user’s identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user’s information on a local operating system or within an authentication server.

Peer entity authentication- is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.

Data – origin authentication- is a property that a message has not been modified while in transit (data integrity) and that the receiving party can verify the source of the message.

Access Control- it is a method of guaranteeing that users are who they say they are and that they have the appropriate access to company data.

Data confidentiality- it is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

Data integrity- is the maintenance of, and the assurance of the accuracy and consistency of data over its entire life-cycle, and is a critical aspect to the design, implementation and usage of any system which stores, processes, or retrieves data.

Non-Repudiation- The non-repudiation service can be viewed as an extension to the identification and authentication service. In general, non-repudiation applies when data is transmitted electronically; for example, an order to a stock broker to buy or sell stock, or an order to a bank to transfer funds from one account to another. The overall goal is to be able to prove that a particular message is associated with a particular individual.

1. 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.