NAME: OKEKE OTITOCHI MARYANN

CSC 418

REVISIED QUESSTION 1

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. 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 subtle reasoning.
3. 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.
4. 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 (Transmission Control Protocol/Internet Protocol) should mechanisms be placed.
5. 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 behavior may complicate the task of developing the security mechanism. For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.
6. 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.
7. 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.
8. Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.
9. 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.
10. 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.
11. Describe the level of security impact in relation to confidentiality, integrity and availability on the following scenario:
12. Student enrollment information
13. Anonymous online poll.
14. Public Web site for a university.
15. Differentiate between data integrity and system integrity.

|  |  |
| --- | --- |
| Data Integrity | System Integrity |
| 1. 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. For example, in an e-commerce system, you will want to make sure that a customer that have purchased an eBook can download it after the payment is issued. If the payment is going through but for some reason the component responsible to allowing the order to complete is not working properly, you will have a system out of sync, and the customer won't be able to download the eBook. Same thing when your system is being hacked, the system integrity is compromised. |
| 1. 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. |

1. Computer and network security are both fascinating and complex, justify.

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.

Because of the point above, the procedures used to provide particular services are often counterintuitive. Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

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

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.

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.

1. Define the following:
2. **Security Attack-** A security attack is an unauthorized attempt to steal, damage, or expose data from an information system such as your website.
3. **Security Mechanism-** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
4. **Security services-** 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.
5. What is computer security? Using relevant examples, describe four key objectives of computer security.

**Computer security**, also known as **cybersecurity** or **IT security**, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

**Key Objectives**

1. Confidentiality- Only authorized users can access the data resources and information.

2. Integrity- Only authorized users should be able to modify the data when needed.

3. Availability- Data should be available to users when needed.

4. Authentication- are you really communicating with whom you think you are communicating with

1. Security attack is classified into two. State and define them.
2. Active Attacks- An Active attack attempts to alter system resources or effect their operations. Active attack involves some modification of the data stream or creation of false statement.
3. Passive Attacks- In a passive attack, an intruder monitors a system and network communications and scans for open ports and other vulnerabilities.
4. What is the goal of a passive attack and active attack?

**Goal of Passive Attack-** Once the intruder has infiltrated the network; they can collect information in a couple of ways. The purpose is solely to gain information about the target and obtain information is being transmitted.

**Goal of Active Attack-** The goal is to alter computer networks and systems resources or alter their operations.

The purpose is solely to gain information about the target and no data is changed on the target.(passiveattack}  
The purpose is to gain information about the target and no data is changed.(active)

1. There are two types of Passive attack, discuss with a given example or scenario.
2. **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.
3. **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.
4. 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. Active attack is classified into four categories, list and discuss using a given example or scenario.

* Replay: An intruder captures communication data and retransmits the captured data for creating unauthorized traffic.
* Masquerade: An intruder pretends to be a legitimate user. This attack is accomplished with some other active attacks.
* Modification of communication content: Some parts of communication content are modified, delayed, or reordered to produce an unauthorized effect.
* Denial of service: This attack prevents normal behaviour of computer networks and systems and services running on these systems. This attack has diverse targets and it is one of the most commonly seen attack types on contemporary computer networks and system.

1. Define Security service as discuss by
2. **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.
3. **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.
4. Define the following:
5. **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.
6. **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.
7. **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.
8. **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.
9. **Data confidentiality-** it is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.
10. **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.
11. **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.
12. Highlights and define four types of confidentiality.
13. **Connection Confidentiality-** The protection of all user data on a connection.
14. **Connectionless Confidentiality-** The protection of all user data in a single data block
15. **Selective-Field Confidentiality-** The confidentiality of selected fields within the user Data on a connection or in a single data block.
16. **Traffic Flow Confidentiality-** The protection of the information that might be Derived from observation of traffic flows.