UBUA VERA

16/SCIO1/048

COMPUTER SCINCE

400 LEVEL

1. Differentiate between these types of integrity:
2. A connection-oriented integrity service

A connection-oriented integrity service is the service that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.

The connection-oriented integrity service addresses both message stream modification and denial of service.

1. Connection Integrity with Recovery

Connection integrity with recovery provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

1. Connection Integrity without Recovery

Connection integrity without recovery

As above, but provides only detection without recovery.

1. Selective-Field Connection Integrity

Selective-field connection integrity provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

1. Selective-Field Connectionless Integrity

Selective-field connectionless integrity Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

1. Define the following:
2. **Nonrepudiation, Origin-** provides the recipient(s) of a message with the proof of the origin of the message. It will protect against any attempt by the originator to falsely deny sending the message.
3. **Nonrepudiation, Destination-** Proof that the message was received by the specified party.
4. **Encipherment-** the process of making data unreadable to unauthorized entities by applying a cryptographic algorithm (an encryption algorithm).
5. **Digital signature-** A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).
6. Authentication exchange-
7. **Routing control-** Route control is a specialized type of network management that aims to improve Internet connectivity, and reduce bandwidth cost and overall internetwork operations.
8. **Notarization-** Notarization is the official fraud-deterrent process that assures the parties of a transaction that a document is authentic, and can be trusted.
9. **Traffic Padding-** this produces ciphertext output continuously, even in the absence of plaintext. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, random data are encrypted and transmitted.
10. **Security Label-** it tells the protocol processing how to handle the data transferred between two systems. That is, the securitylabel indicates what measures need to be taken to preserve the condition of security.
11. Define the following:
12. **Plaintext-**it is a term used in cryptography that refers to a message before encryption or after decryption. That is, it is a message in a form that is easily readable by humans. Encryption is the process of obscuring messages to make them unreadable in the absence special knowledge.
13. **Ciphertext-** ciphertext or cyphertext is the result of encryption performed on plaintext using an algorithm, called a cipher. Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it.
14. **Encryption-** encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext.
15. **Decryption-** the inverse of encryption, is the process of turning ciphertext into readable plaintext.
16. **Cryptography-** this is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
17. **Cryptanalysis-** Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break into cryptography or information security systems.
18. **Cryptology-** The study of cryptography and cryptanalysis.
19. **Cryptosystem-** A particular suite of algorithms and protocols for encryption, decryption, and key generation. Examples: Cramer-Shoup cryptosystem, Rabin cryptosystem, Benaloh cryptosystem, RSA cryptosystem.
20. Symmetric encryption scheme has five ingredients; state and discuss.
21. **Plaintext-** The term **plaintext** refers to the original message that is created and sent into the encryption method; since you're bothering to encrypt it, the plaintext most likely contains sensitive data that should not be seen by prying eyes.
22. **Encryption Algorithm-** The algorithm takes the plaintext and converts it into an unreadable format. A simple example of an encryption algorithm would be changing all Ns to a 3, or all Zs to a 1. The routine may perform several passes and changes, called permutations, on the plaintext. Once it's encrypted, you'll need a key to unlock it.
23. **Key-** Think of the **key** as a decoder ring: the secret of the scrambled text cannot be read without the key. The key holds the information on all the switches and substitutions made to the original plain text.

In symmetric encryption, the key is actually bundled with the algorithm; in this sense, the decoder ring is not universal. The changes and substitutions depend on the key, and vice versa because the sender and recipient share the key.

1. **Ciphertext**- The **ciphertext** is the text that is now scrambled and ready to be sent. It may look like a random stream of data, and is unreadable.
2. **Decryption Algorithm-** In the decryption algorithm, the secret key (the decoder ring) is applied to the ciphertext. It converts it back to plaintext, basically performing the encryption in reverse.
3. What are two requirements for secure use of conventional encryption?

1. The encryption algorithm must be strong- At a minimum, an opponent who knows the algorithm and has access to one or more ciphertexts would be unable to decipher the ciphertext or figure out the key. In a stronger form, the opponent should be unable to decrypt ciphertexts or discover the key even if he or she has a number of ciphertexts together with the plaintext for each ciphertext.

2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm, all communication using this key is readable.

1. Discuss four key objectives of cryptography. Or four key objectives of cryptography
2. **Confidentiality-** Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft. Confidentiality has to do with the privacy of information, including authorizations to view, share, and use it. Information with low confidentiality concerns may be considered "public" or otherwise not threatening if exposed beyond its intended audience. Information with high confidentiality concerns is considered secret and must be kept confidential to prevent identity theft, compromise of accounts and systems, legal or reputational damage, and other severe consequences.
3. **Integrity-** 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. The term is broad in scope and may have widely different meanings depending on the specific context – even under the same general umbrella of computing. It is at times used as a proxy term for data quality, while data validation is a pre-requisite for data integrity. Data integrity is the opposite of data corruption.
4. **non-repudiation-** is the assurance that someone cannot deny something. Typically, **nonrepudiation** refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
5. **Authentication-** Authentication is a technique used to verify that someone is who they claim to be. Authentication isn’t sufficient by itself to protect data, Crowley notes. What’s needed is an additional layer, authorization, which determines whether a user should be allowed to access the data or make the transaction they’re attempting.
6. Discuss symmetric algorithm.

Symmetric key algorithms are sometimes referred to as secret key algorithms. This is because these types of algorithms generally use one key that is kept secret by the systems engaged in the encryption and decryption processes. This single key is used for both encryption and decryption. Symmetric key algorithms tend to be very secure. In general, they are considered more secure than asymmetric key algorithms. There are some symmetric key algorithms that are considered virtually unbreakable. Symmetric key algorithms are also very fast. This is why they are often used in situations where there is a lot of data that needs to be encrypted. In symmetric key algorithms, the key is shared between the two systems. This can present a problem. You have to figure out a way to get the key to all systems that will have to encrypt or decrypt data using a symmetric key algorithm. Having to manually distribute a key to all systems can be a quite cumbersome task. Sometimes, this can only be done by copying the key from a central location.

1. What is a compromise?

It is the possibility that the security of an encryption algorithm is at risk at a cost that is lower than initially assumed.

1. Give another name for attempted cryptanalysis.
2. Discuss four general types of cryptanalytic attack. Or four general types of cryptanalytic attack are
3. **Ciphertext-only attack-** The only information the cryptanalyst has to work with is the ciphertext of various messages all encrypted with the same algorithm.
4. **Known-plaintext attack-** In this scenario, the cryptanalyst has access not only to the ciphertext of various messages, but also the corresponding plaintext as well.
5. **Chosen plaintext attack-** The cryptanalyst has access to the same information as in a known plaintext attack, but this time may choose the plaintext that gets encrypted. This attack is more powerful, as specific plaintext blocks can be chosen that may yield more information about the key. An adaptive-chosen-plaintext attack is merely one where the cryptanalyst may repeatedly encrypt plaintext, thereby modifying the input based on the results of a previous encryption.
6. **Adaptive-chosen plaintext attack-** this is a chosen plaintext attack scenario in which the attacker has the ability to make his choice of the inputs to the encryption function based on the previous chosen plaintext queries and their corresponding ciphertexts. The scenario is clearly more powerful than the basic chosen plaintext attack, but is probably less practical in real life since it requires interaction of the attacker with the encryption device.