Namrata Maurya
TYIT - B
20698

ASSIGNMENT-1

SECURITY IN COMPUTING

Q1] Differentiate between Lollipop model & onion model.

Ans:-

Lollipop Model	Onion Model.
• Also known as perimeter security	• Also known as defense in depth.
• involves building a single wall around the objects of value.	• Has multiple layers of wall around the objects of value.
• It is like a lollipop with hard crunchy shell on outside & soft on the inside	• It is like a onion with multiple layers & plenty of crying while peeling each layer.
• Fails do address inside threats & provides no protection against a perimeter breach.	• A layered security architecture provides multiple levels of protection against Internal & external threats.
• Firewall is the only network security strategy	• There are more layers rather than firewall which also shows better protection against threats.

Q2] Differentiate between authentication and authorization.

Ans:-

Authentication	Authorization.
• In authentication process, the identity of users are checked for accessing the system.	• In authorization process, users authorities are checked for accessing resources.
• users are verified	• users are validated.
• Done before the authorization process	• done after the authentication process
• usually need user's login credentials	• needs user's privilege or security levels
• determines whether the person is user or not	• determines what permission do user have?
• Transmits info through ID token	• transmits info through an Access token
• eg. Employees in a company are required to authenticate through the network before accessing their company email	• eg. After an employee successfully authenticates, the system determines what info the employees are allowed to access.

Q3] Write down the steps performed to create Digital signature & explain it with proper example.

Ans:- • A digital signature is a mathematical technique used to validate the authenticity & integrity of a message, s/w or digital document.

• Steps to create digital signature:-

① Message digest is computed by applying hash function on the message & then message digest is encrypted using private key of sender to form the digital signature.

② Digital signature is then transmitted with the message.

③ Receiver decrypts the digital signature using the public key of sender

④ The receiver now has the message digest

⑤ The receiver can compute the message digest from the message.

⑥ The message digest computed by receiver & the message digest need to be same for ensuring integrity.

- To create a digital signature, signing algorithms like email programs create a one-way hash of the e-data which is to be signed.
- The signing algo then encrypts the hash value using private key.
- This encrypted hash along with other info like the hashing algo is the digital signature.
- This digital signature is appended with data & sent to the verifier.
- The reason for encrypting the hash instead of entire ~~hash~~ message is that a hash function converts any arbitrary input into a much short or fixed value.

04] Differentiate between public key cryptography & private key cryptography.

Private key	Public key
• Private key is faster than public key	• It is slower than private key.
• the same key & algo is used to encrypt & decrypt the message	• 2 keys are used, one key used for encryption & other for decryption.
• The key is kept as a secret.	• one of the 2 keys is kept as a secret.
• Private key is symmetrical because there is only one key that is secret key	• Public key is asymmetrical because there are 2 types of keys private & public.
• Sender & receiver need to share the same key	• Sender & receiver does not share the same key.
• Performance testing checks the reliability, scalability & speed of the system.	• Load testing checks the sustanibility of the system.

05] Write a short note on PKI.

Ans:- Public Key Infrastructure (PKI) is a technology for authenticating users & devices in the digital world. The basic idea is to have one or more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device. The key can then be used as an identity for the user in digital networks.

The users & devices that have keys are often just called entities. In general, anything can be associated with a key that it can use as its identity. Besides a user or device, it could be a program, process, manufacturer, component, or something else. The purpose of a PKI is to securely associate a key with an entity.

A ~~pub~~ PKI relies on digital signature technology, which uses public key cryptography. The basic idea is that the secret key of each entity is only known by that entity & is used for signing. This key is private key. There is another key derived from it called public key which is used for verifying signatures.