Jessica Braganza
BE Comp 2
F17112151

PAGE NO :
DATE :

ICS Assignment 2

1) Explain the working of Diffie-Hellman key exchange algorithm.

Ans. Diffie Hellman (DH) key exchange algorithm is a method for securly exchanging cryptographic key over a public communication channel. Keys are not actually exchanging - they are jointly derived.

- If Alice and Bob wish to communicate with each other, they first agree between them a large prime number (P) and a generator (g) where (0 < g < P)
- Alice chooses a secret integer 'a' (her private key) and calculates g^amodp (which is her public key).
- Bob chooses his private key 'b' and calculates his public key.
- Bob knows b and g^a, so he can calculate (g^a)^b mod p. Therefore, both Alice and Bob know a shared secret g^ab mod p.
- An eavesdropper, Eve, who was listening in on the communication knows p, g, Alice's public key (g^a mod P) and Bob's public key (g^b mod P), she is unable to calculate shared secret from these values.
- In static mode, both Alice and Bob retain their private or public keys over multiple communications.
- Therefore the resulting shared secret will be the same every time.
- In emphemeral static mode, one party will generate a new public/private key every time. Thus new shared secret will be generated.

2) What is kerberos? Explain in detail.

Ans. - Kerberos provides a centralized authentication server whose function is to authenticate user to servers and servers to users.

- In Kerberos authentication, server and database is used for client authentication.
- Kerberos runs as a third party trusted server known as the Key distribution center (KDC).

- Each user and service on the network is a principle.

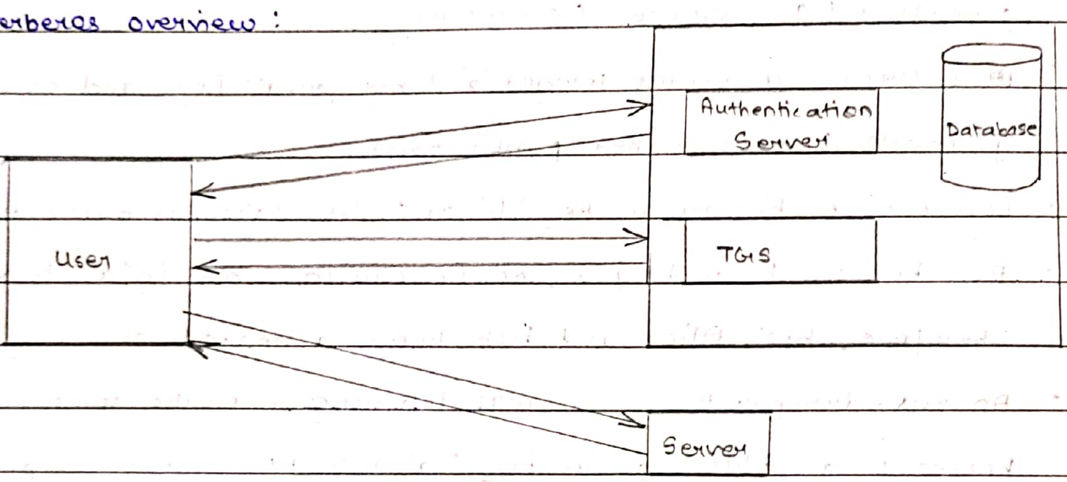
The main component of kerberos are:

i) Authentication Server (AS) : The authentication server performs the initial authentication and ticket for ticket granting service.

ii) Database : The authentication server verifies access right of user in database.

iii) Ticket Granting server (TGS) : The TGS issues the ticket for the servers.

kerberos overview :



Step 1 : user login and request services on host. Thus user request for ticket granting service.

Step 2 : Authentication server verify user access right using database and then gives ticket-granting and session key. Results are encrypted using password of user.

Step 3 : Decryption of message is done using the password, then send the ticket to TGS. The ticket contain authenticator like username and network address.

Step 4 : The TGS decrypts the ticket sent by user and authenticator verify the request then creates the ticket for requesting services from server.

Step 5 : User sends the ticket and authenticator to the server.

Step 6 : Server verify the ticket and the authenticator, then generate access to ~~servi~~ services. After this user can access these services.

3) Write short note on SSL Protocols.

Ans. 1) Secure socket layer (SSL) is a standard protocol used for secure termination of the document over network.

2) SSL technology creates a secure link between web server and browser to ensure private integral data transmission.

3) SSL uses transport control protocol for communication.

4) In SSL, the work socket refers to the mechanism of transferring data between client and server over a network.

5) When using SSL for secure Internet transaction, a web server needs an SSL certificate to establish a secure SSL connection.

6) SSL encrypts network connection segment above transport layer, which is network connection component above the program layer.

7) SSL follows asymmetric cryptographic mechanism, in which web browser creates a public key and a private key.

8) The public key is placed in a data file known as a certificate signing request.

9) The private key is issued to a recipient only.

10) The objective of SSL are:

i) Data integrity: Data is protected from tampering.

ii) Data privacy: Data privacy is ensured through a service of protocol, including SSL protocols, SSL handshake protocol, SSL change cipher protocol.

iii) Client-server authentication: The SSL protocol uses standard cryptography technique to authenticate client and server.

11) SSL is the predecessor of the Transport layer security (TLS), which is cryptographic protocol for secure internet data transmission.