One-way and mutual authentication schemes

One - Way Authentication

One Way authentication refers to the authentication of only one end of the communication.

For example, if there are 2 users A and B who want to communicate with each other. In this scheme User A is the client and User B is the server. Suppose User B wants to authenticate user A before the actual communication, but user A is not able to authenticate the server before the communication begins. Such a scheme is called a One Way Authentication Scheme or Protocol.

There could be multiple factored authentication mechanisms used to provide much better security. for example a 2 Factor authentication, which depends upon a password and a 4 digit PIN to validate the authentication process.

But Dont confuse this with mutual authentication. Over here only the client is getting authenticated to the server using multi factor authentication.

One-way and mutual authentication schemes

Mutual Authentication

Mutual Authentication is a mechanism to authenticate both the entities involved in the communication process, ie. the sender and the receiver or client and server.

The sender must prove its identity to the receiver and vice versa before the actual communication could even begin.

One-way and mutual authentication schemes

In order to achieve mutual authentication, there must be certain provisions of some protocols which suppose to verify identity of the sender over an insecure communication channel.

To achieve this goal , most of the protocols depend upon an authentication server also called as the Key Distribution Center (KDC).

Ticket , Session Key

If the sender A wants to communicate with receiver B, then A can request for a session key from the Key Distribution Center(KDC) for communicating with B. These Authentication servers are capable of delivering good quality random session keys and distribute them securely to the clients who request it.

These Authentication servers also maintain a table containing the name and master key or secret key of each client.

The secret keys are used to authenticate the clients to the authentication servers and then for secure transmission of data between the client and the authentication servers.