Internet Authentication

– Internet Authentication is needed because environments now consist of many servers, each with its own concerns

➢ Kerberos
  • Third party system to authenticate a user at log-in. The authentication is done at a per “realm” (services subset) basis.
  • The authentication process is as follows:
    1) The user sends a request for a Ticket-Granting Ticket to the Kerberos authentication server
    2) The server sends back a ticket that is formed with the users password (or some derivation), and a session key
    3) The user then sends a request for a Service-Granting Ticket to the ticket granting server
    4) The server sends back a ticket specific to the service requested and a session key for that service.
    5) When the user tries to connect to the service, that user can be verified by using the ticket
  • Authentication can be shared between realms if there is trust between realms

➢ X.509
  • Uses a public-private key system
  • The Certificate Authority stores public keys from all the services that have bought certificates
  • The certificate can then be verified and the entities public key can be used
    • Each time the certificate is used, it should be checked to make sure it is still valid (i.e. has not been removed or changed)