Kerberos: Internet authentication – allows authentication to servers
- Most used internet authentication system
- Enforcing least privilege in cloud systems
- Requires user to prove identity for each service used/invoked

How Kerberos Authenticates:
- Uses tickets encrypted with password/derivative to authenticate
- Sends ticket to authenticating server which decrypts and compares
- Shared private key between service server and authenticating server
- Ticket granting ticket & service granting tickets used
- Never sends password over the wire (just used as input to encryption algorithm)

Kerberos Realm:
- Authenticating server in a realm knows about all servers and clients in the realm
- Application servers share keys with Kerberos server
- Ex: the CS department and ECE departments are separate realms
- For authentication between multiple realms (inter-realm): participating servers must be willing to trust other Kerberos server (shared keys)

X.509: Digital Certificates
- Two key system: public/private keys
- Get/give public key from/to CA (certifying authority)
- Problems with CA: masquerading
- To authenticate CA, CA signs certificate with private key, decrypt with CA's public key
- If need to reissue private keys, revoke certificates with the private key. Clients check if certificate is valid through the CA
- Used in IPsec, SSL, SET, S/MIME etc.

Public-Key Infrastructure (PKI/PKIX):
- Manages keys/certificates
- Includes, creation, management, storage, distribution and revoking of digital certificates based