Topic: Digital Certificates/Authentication

* Digital certificate proves authenticity of an endpoint/user by using cryptography and using the public key infrastructure
* Makes sure that only authorized users/devices can use a service or access/connect a network
* Digital certificates also prove authenticity of websites which can also be called a SSL certificate
* Contains identifiable information
  + Name, company department, IP address/serial number
* Contains a public key which must be verified using it’s matching private key
* Issued by certificate authorities (CA) that sign certificate to verify who the user or device is
  + They manage domain control verification and make sure the public key with the certificate belongs to the user/organization

Types

* Transport layer security TLS/SSL certificate
  + Stays on server to make sure client communication is private and encrypted
  + Authentication for server and makes server able to receive encrypted messages from clients
  + This certificate is present with HTTPS at beginning of URL
  + Three forms:
    - Domain validated: quick and acceptable for any website and cheap
    - Organization validated: light business authentication typically for selling online products
    - Extended validation: full business authentication and required by large organizations and business handling sensitive info. Highest level of authentication and security
* Code signing certificate
  + Developer or publisher signs software to prove the authenticity of it or files downloaded off the internet
  + Used to confirm that it is genuine and hasn’t been altered
* Client certificate
  + Identifies a user or machine for another user or machine. Used for email encryption and to access sensitive resources (like databases)

Benefits

* Security: encrypt internal/external data as well as communications so that an attacker cannot access/intercept data
* Scalability: provides everyone with the same encryption quality and can quickly be issued, revoked, and renewed
* Authenticity: verifies the authenticity of online communication in a time where cyber threats are constantly present. Make sure that messages always and only reach their end recipient.
* Reliability: Only publicly trusted CA’s can issue digital certificates through a rigorous process so that attackers cannot obtain one to take advantage of unknowing users.
* Public Trust: proves a site is genuine or that emails/documents are authentic and proves to users that the sender can be trusted

Digital certificate vs. digital signature

* DC: verifies identity and encrypts connections
* DS: hashes using numeric string to authenticate and documents and identity. DS is usually attached to a document or email with a cryptographic key, after which the signature is hashed and the recipient authenticates by performing the same hashing function to decrypt it

https://www.fortinet.com/resources/cyberglossary/digital-certificates#:~:text=A%20digital%20certificate%20is%20a,can%20connect%20to%20their%20networks.