Date / /
Page No.

Kerberos

It is a network authentication protocol that provides secure and reliable authentication between client and servers. It designed to prevent unauthorized access and protect against various security threats such as evasdropping or replay attack.

Kerberos is a system that allows users and services to ~~provide~~ securely prove their identities to each other over a network using cryptographic authentication ~~tokens~~ tickets. It ensures that only authorized users can access resources and helps to protect sensitive information from unauthorized access.

It uses symmetric key cryptography and a trusted-third party authentication server.

X.509

X.509 is widely accepted standard that defines the format and structure of digital certificates used in secure communication. These certifications ~~are~~ are electronic documents that contains information of an entity such as an individual, organization or device along with their corresponding public key.

X.509 certificates are issued by certificate authorities and plays a crucial role in establishing trust, facilitating authentication, enabling encryption and ensuring data integrity

They form a hierarchical trust chain with root CAs at the top, intermediate CAs in the middle and end-entity certificates at the bottom.
X.509 certificates are widely used in protocols like SSL/TLS to secure web communications (HTTPS) and S/MIME for secure email communication providing a trusted framework for secure online transactions and data exchange.

Secure Socket Layer (SSL) & Transport layer Security (TLS)

SSL/TLS

SSL/TLS is a cryptographic protocol that provides secure communication over networks. It establishes an encrypted and authenticated connection between client and servers, ensuring the confidentiality, integrity and authenticity of data transmitted between them.

It encrypts data to ensure it remains private and unreadable to unauthorized parties

It verifies the integrity of data to detect any tampering or modification

It provides authentication to verify the identities of communicating parties

It uses digital certificates issued by trusted CA

It is commonly used with HTTP to create HTTPS for secure web browsing

It protects sensitive information like passwords and credit card details.

It establish a secure connection through a handshake protocol.

It has evolved into newer versions like TSL 1.2 and TSL 1.3

It plays a crucial role in securing online transactions and protecting users privacy.