TRANSPORT LAYER SECURITY (TLS).

Presented by : Jenil Arvindbhai Paladiya

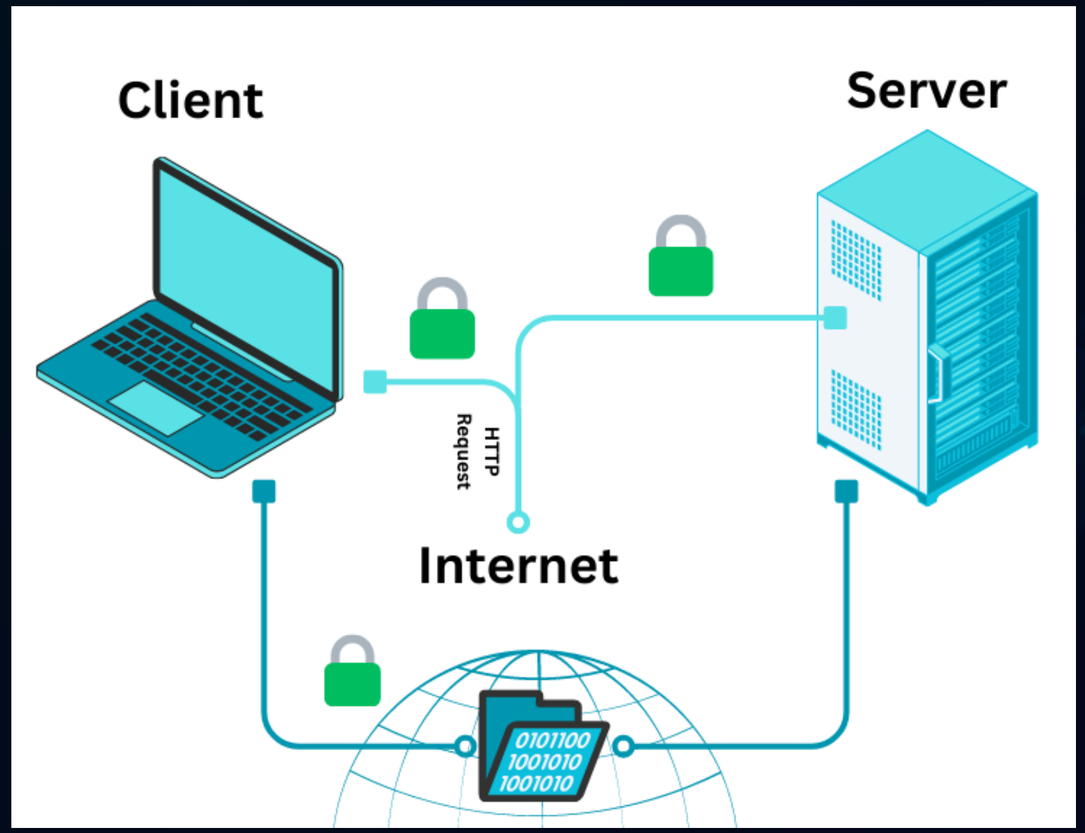
Matriculation Number : 4243558

INDEX

OVERVIEW OF TLS AND ITS MAIN COMPONENTS

Definition: TLS (Transport Layer Security) is a cryptographic protocol that ensures secure communication over the internet by encrypting data between devices.

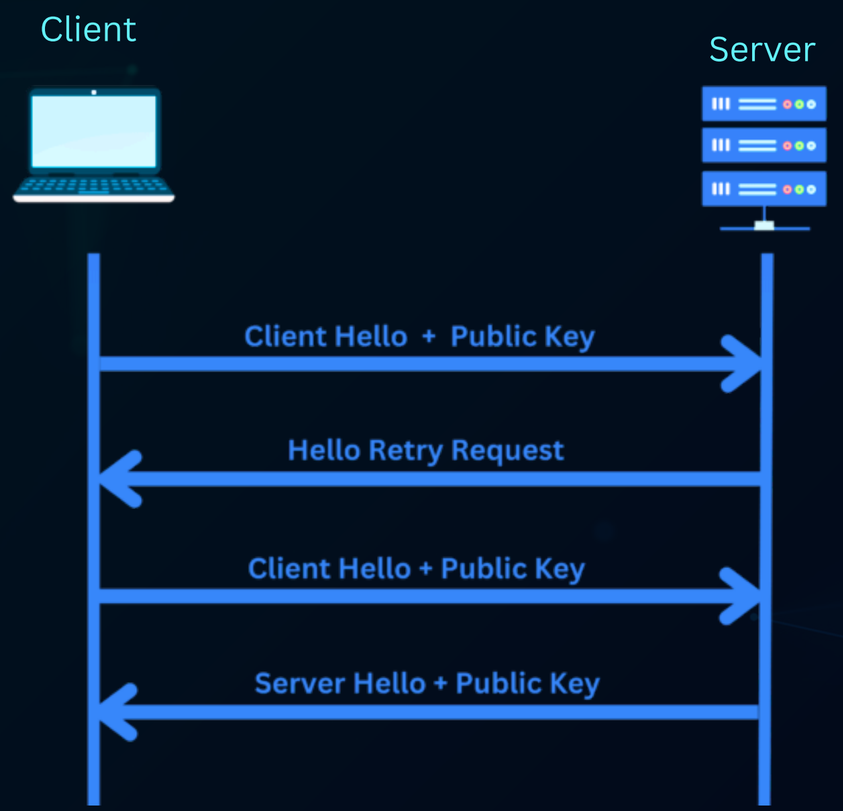
1. Encryption
   - Function: Encrypts the data, ensuring that no one can read it during transmission.
2. Authentication
   - Function: Verifies the identity of the communicating parties, ensuring the right server is being communicated with.
3. Data Integrity
   - Function: Ensures that data is not tampered with during transmission, maintaining its authenticity.
4. Session Keys
   - Function: Uses temporary, symmetric keys for faster encryption during a session.



HOW TLS WORKS (HANDSHAKE PROCESS)

Step 1: Client Hello

- The client initiates the handshake by sending supported TLS versions, cipher suites, and other relevant parameters to the server.



Step 2: Server Hello

- The server responds with its chosen configuration and sends a digital certificate to authenticate its identity.

Step 3: Certificate Verification

- The client checks the server's certificate to verify its authenticity, ensuring it's signed by a trusted Certificate Authority (CA).

Step 4: Key Exchange

- Both the client and server exchange keys (using asymmetric encryption) to securely generate a session key for further communication.

Step 5: Secure Communication

- Encrypted data transfer begins using the session key for encryption and decryption, ensuring confidentiality and integrity of data.

MAIN SERVICES WHERE TLS IS APPLIED

Service Type	Example	Icon/Image
Web Browsing	HTTPS secure websites	
Email Services	IMAP, SMTP encryption	
Online Payments	E-commerce payment gateways	
VPN Connections	Secure tunneling for remote workers	
VoIP Services	Encrypted voice communication	

CRYPTO ALGORITHMS USED IN TLS AND THEIR SELECTION

Algorithm Type	Example	Purpose	Icon/Image
Key Exchange	ECDHE	Secure key generation	
Encryption Algorithm	AES-128, AES-256	Encrypting	
Hashing Algorithm	SHA-256	Ensures data integrity	
Digital Signature	RSA, ECDSA	Certificate validation	

LIMITS OF TLS

While TLS provides robust security, there are certain limitations and challenges that can impact its effectiveness.

Data Security (Encrypts sensitive information)

User Trust (Secure websites display a padlock icon)

Authentication (Verifies server identity)

Defense Against Attacks (Prevents man-in-the-middle (MITM) attacks)

LIMITS OF TLS

While TLS provides robust security, there are certain limitations and challenges that can impact its effectiveness.

Performance Overhead (Slight delay due to encryption processes)

Certificate Management (Expired or mismanaged certificates disrupt security)

Limited Protection Scope (website stores passwords without encryption)

Configuration Issues (Poor server setup can weaken security)

REAL-WORLD EXAMPLES AND CASE STUDY

Case Study (2014 – Google’s Priority on HTTPS):

- Case Study Overview: In 2014, Google announced that websites using HTTPS (secured by TLS) would receive a ranking boost in search results. This move incentivized website owners to adopt TLS for improved security and better SEO performance.

1. E-commerce (🛒):
   - E-commerce websites use TLS to protect customer transactions. TLS ensures that sensitive information such as credit card details and shipping addresses are encrypted during the checkout process.
2. Banking (💳):
   - Banking websites use TLS to provide secure access to financial accounts. It encrypts login credentials, transaction details, and other sensitive data to ensure privacy and prevent hacking.
3. Social Media (📱):
   - Social media platforms like Facebook and Twitter use TLS to secure logins and communication. This protects users' personal data and messaging from unauthorized access, especially on public networks.

Impact: This decision significantly influenced the internet landscape, accelerating the adoption of HTTPS across the web and making secure connections a standard practice for many websites, from blogs to large e-commerce platforms

CONSLUSION

TLS ensures that online communication is secure by encrypting data, verifying identities, and ensuring data integrity

- Summary: TLS plays a critical role in ensuring secure communication on the internet by encrypting data, authenticating parties, and maintaining data integrity.
- Final Note: Continuous upgrades and proper configurations are essential for its effectiveness.
- Call to Action: "Ensure your systems use the latest TLS version and secure configurations!"

Studio Shodwe

THANK YOU