19Z701 - Cryptography

Transport Layer Security

Gokul G - 22z221
Hariharan D - 22z222
Harish K - 22z223
Pranavji K - 22z245
Rajailakkiyan I B- 22Z250
Sibi Senthil - 22Z280

INTRODUCTION TO SECURE COMMUNICATION

Hariharan D – 22z222

What is TLS ?

- TLS (Transport Layer Security) is a cryptographic protocol
- Ensures secure communication between web browsers, apps, and servers
- It’s the “S” in HTTPS (HyperText Transfer Protocol Secure)
- Protects data from being exposed during transmission

The Problem – Why Do We Need Security?

The Internet was originally designed for openness, not security

Risks without TLS:

- **Eavesdropping** (attackers listening to traffic)
- **Data Theft** (passwords, credit cards stolen)
- **Data Tampering** (hackers altering information in transit)
- **Impersonation** (fake websites pretending to be real ones)
- Example: Without HTTPS, entering bank details online is unsafe

The Three Core Goals of TLS

1. **Encryption**
   - Keeps data private (only sender & receiver can read it)
2. **Authentication**
   - Ensures you're talking to the real website/server, not an imposter
3. **Integrity**
   - Protects against data tampering during transfer
   - Ensures information received = information sent

TLS HANDSHAKE – ESTABLISHING TRUST

Pranavji K – 22z245

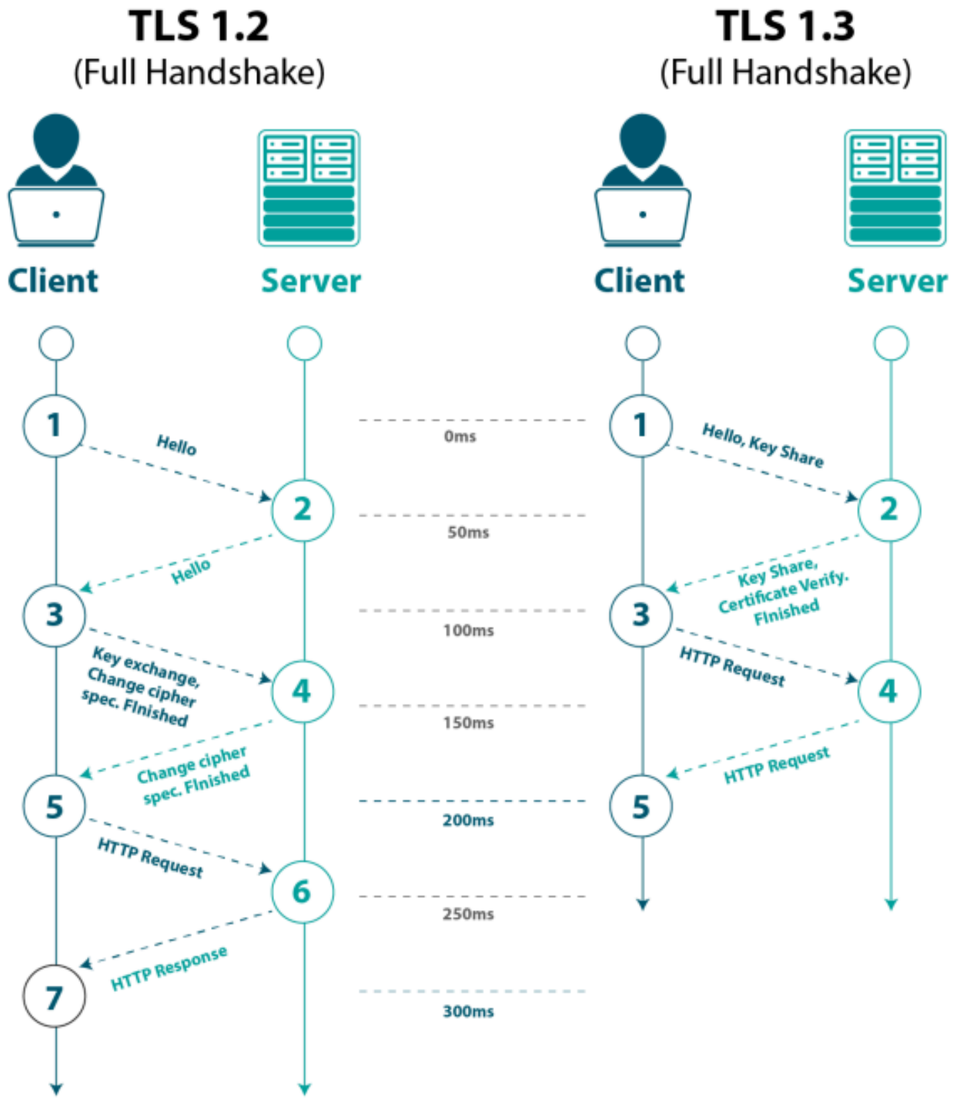
What is the TLS Handshake?

- A digital introduction between client and server
- Ensures trust before exchanging any sensitive data
- The client and server exchange messages to establish a secure connection.
- They agree on encryption methods, verify identities, and generate session keys.

TLS 1.2 Handshake

1. **Client Hello:** Client proposes TLS version, cipher suites, and random data.
2. **Server Hello:** Server selects the version and cipher suite, then sends its certificate.
3. **Key Exchange & Certificate Verification:** Server and client exchange keys (e.g., RSA/Diffie-Hellman).
4. **Change Cipher Spec & Finished:** Both confirm encryption parameters and finalize handshake.

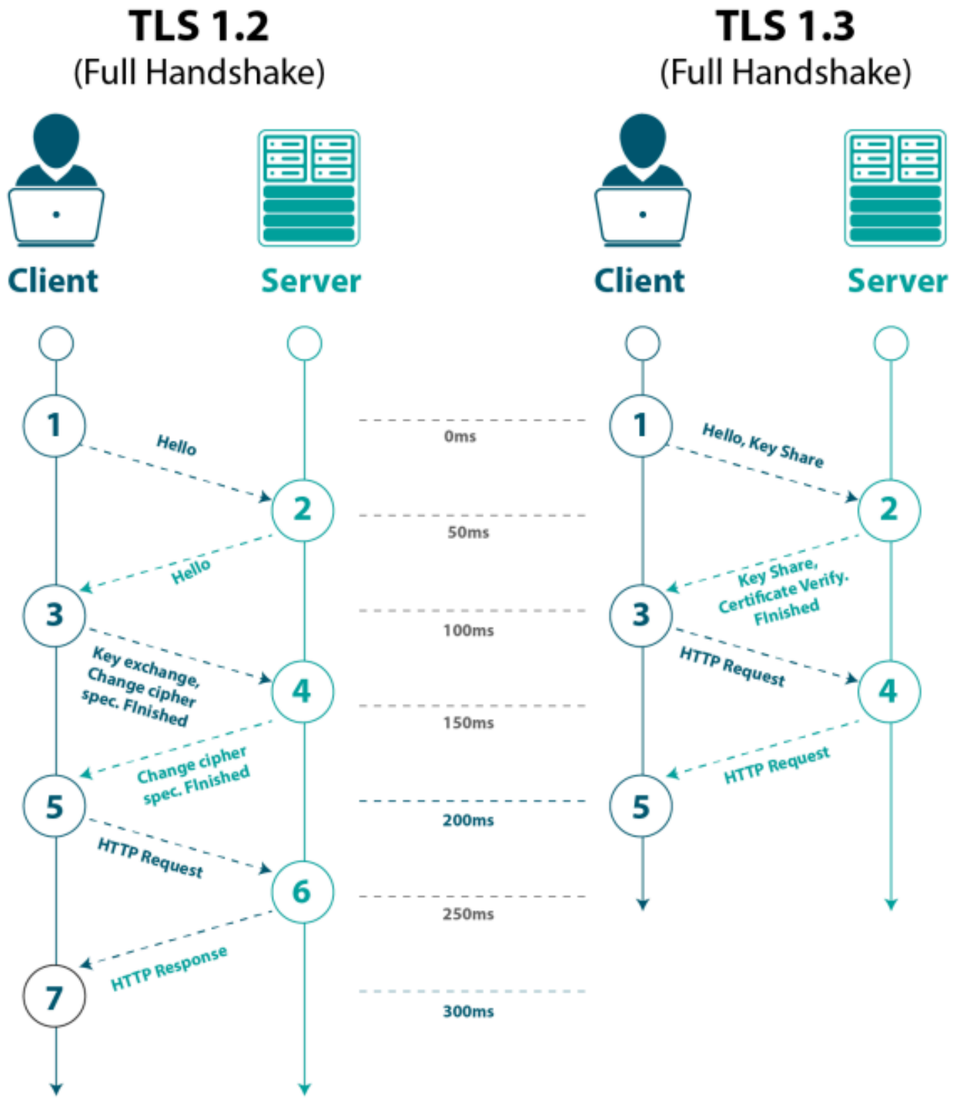
Latency: Takes **two round trips** (client ↔ server ↔ client) before encrypted data transfer begins.



TLS 1.3 Handshake

1. **Client Hello:** Client sends supported parameters and an initial key share immediately.
2. **Server Hello:** Server replies with chosen cipher suite and its key share.
3. **Certificate Verify & Finished:** Server proves its identity and completes the handshake.
4. **Encrypted Communication Begins:** Client can send HTTP request immediately after one round trip.

Improvement: TLS 1.3 reduces the handshake to **one round trip**, making it **faster** and **more secure** than TLS 1.2.



THE CRYPTOGRAPHY BEHIND TLS

Sibi Senthil – 22z280

The Backbone of TLS – Cryptography in Action

- TLS uses cryptography to secure internet communication.
- Combines asymmetric and symmetric encryption for efficiency and security.
- Ensures the 3 pillars: Confidentiality, Authentication, and Integrity.
- Cryptography transforms readable data into secure code — only authorized parties can decode it.

How TLS Uses Both Encryption Types

- **Symmetric Encryption:** Same key for encryption and decryption — used for speed.
- **Asymmetric Encryption:** Uses public and private key pair — ensures secure key exchange
- **Algorithms:** AES, ChaCha20 (Symmetric) | RSA, Diffie-Hellman, ECDHE (Asymmetric)
- TLS uses asymmetric encryption during handshake, then switches to symmetric for data transfer.

THE PILLARS OF TLS SECURITY

Gokul G – 22z221

Pillar	What It Is (The Goal)	How It Works (The Method)	The Result (The Protection)
Encryption (Keeping Data Private)	The "secrecy" part. Ensures no one can "listen in" on your conversation.	All data (passwords, search queries, etc.) is scrambled using the **Symmetric Session Key** that was created during the handshake.	An attacker who intercepts the data only sees meaningless, unreadable garbage, not your sensitive information.
Authentication (Verifying Identity)	The "trust" part. It's how you know the server you're talking to is *actually* who it claims to be.	This is handled during the handshake using the **Digital Certificate**. Your browser verifies the certificate was issued by a trusted **Certificate Authority (CA)**.	Prevents **"Man-in-the-Middle" (MitM) attacks**, where an attacker impersonates a real website (like your bank) to steal your data.
Integrity (Protecting Data from Tampering)	The "genuineness" part. It ensures the data you *receive* is the *exact* same data that was *sent*, with no modifications.	TLS uses a **Message Authentication Code (MAC)**—like a "digital wax seal." This is a unique signature for each message, created using the Session Key.	Your browser receives the message, calculates its own MAC, and compares it to the one sent. If they don't match, the data is rejected, protecting you from altered data.

TLS IN ACTION & ITS EVOLUTION

HARISH K

22Z223

Evolution Timeline of TLS

- SSL 2.0 (1995): First attempt at web security (now obsolete)
- SSL 3.0 (1996): Fixed major flaws but later deprecated
- TLS 1.0 (1999): Based on SSL 3.0 – first official version
- TLS 1.1 (2006): Improved resistance to CBC attacks
- TLS 1.2 (2008): Introduced modern ciphers (SHA-256, AEAD)
- TLS 1.3 (2018): Simplified handshake, improved speed, stronger security

TLS 1.3 is now the standard for secure communication — it's faster, more private, and more resistant to known attacks.

Improvements in TLS 1.3

- **Faster Handshake:** Only 1 round trip → reduces latency
- **Forward Secrecy by Default:** Uses ephemeral keys (no reuse)
- **Removed Weak Algorithms:** Dropped RSA key exchange, MD5, SHA-1
- **Encrypted Handshake:** Even the handshake messages are encrypted
- **0-RTT Mode:** Enables instant session resumption

TLS in Action

TLS in Today’s Internet

- 95%+ of web traffic today is encrypted with TLS (source: Google Transparency Report)
- Most websites automatically redirect HTTP → HTTPS
- Certificate automation via Let’s Encrypt has made HTTPS free and easy
- Browsers now warn users about insecure HTTP sites

FUTURE OF TLS & SUMMARY

RAJAILAKKIYAN I B

22Z250

Emerging Technologies: QUIC, HTTP/3 & Post-Quantum TLS

- QUIC Protocol: Built over UDP; integrates TLS 1.3 for faster, secure connections.
- HTTP/3: Uses QUIC + TLS for reduced latency and improved performance.
- Post-Quantum TLS: Future TLS versions aim to resist attacks from quantum computers using new algorithms (e.g., Kyber, Dilithium).

TLS in the Cybersecurity Ecosystem

- TLS acts as the foundation of trust across digital communications.
- It protects not just browsers, but also APIs, mobile apps, IoT, emails, and VPNs.
- Works alongside other security layers like firewalls, intrusion detection, and identity management.

Best Practices for Strong TLS Deployment

- Use modern versions (TLS 1.3) only.
- Enable Perfect Forward Secrecy (PFS) using ephemeral keys.
- Enforce HSTS (HTTP Strict Transport Security) for HTTPS-only communication.
- Regularly update and renew digital certificates

Summary: Why TLS Remains the Cornerstone

- Ensures confidentiality, integrity, and authenticity online.
- Powers secure experiences — from banking and messaging to e-commerce.
- TLS continues to evolve with technology, remaining the backbone of secure communication in the digital era.