# Researching

Searching for \*\*Funktionsweise von TLS\*\*

Searching for \*\*Hauptkomponenten von TLS\*\*

Searching for \*\*Wichtigste Dienste von TLS\*\*

# Forschungsbericht: Transport Layer Security (TLS)

## Wie funktioniert TLS?

TLS, kurz für Transport Layer Security, ist ein Verschlüsselungsprotokoll, das für die sichere Kommunikation im Internet konzipiert wurde. Es wird vor allem für die Absicherung von HTTPS-Verbindungen genutzt, kommt aber auch in anderen Anwendungen wie E-Mail, Instant Messaging und Voice over IP zum Einsatz.

Der Ablauf von TLS beginnt mit dem Aufbau einer Verbindung vom Client zum Server, wobei zuerst das TLS Handshake Protocol aktiv wird. Dieses Protokoll ermöglicht es Server und Client, einen Verschlüsselungsalgorithmus auszuwählen und sich gegenseitig zu authentifizieren, bevor die eigentlichen Daten übertragen werden. Im Rahmen des Handshakes findet ein sicherer Schlüsselaustausch statt, und es werden die Sicherheitsparameter für die Sitzung ausgehandelt.

Nachdem die Parameter festgelegt sind, kommt das TLS Record Protocol zum Einsatz. Es nimmt die zu sendenden Nachrichten, unterteilt sie in Blöcke, wendet einen Message Authentication Code (MAC) an, verschlüsselt die Daten und sendet sie dann ab. Die Verschlüsselung erfolgt dabei mit einem symmetrischen Schlüssel, der im Handshake ausgehandelt wurde.

TLS verwendet sowohl symmetrische als auch asymmetrische Kryptographie. Asymmetrische Kryptographie wird für den sicheren Austausch des Sitzungsschlüssels verwendet, während die eigentliche Datenübertragung mit einem symmetrischen Schlüssel verschlüsselt wird, der für beide Kommunikationspartner bekannt ist.

Die neueste Version, TLS 1.3, wurde 2018 veröffentlicht und bringt bedeutende Verbesserungen mit sich. Sie trennt Schlüsselvereinbarung und Authentifizierungsalgorithmen von den Cipher Suites, entfernt schwache und wenig genutzte elliptische Kurven und schreibt Perfect Forward Secrecy vor.

## Hauptkomponenten und wichtigste Dienste von TLS

TLS besteht aus zwei Hauptkomponenten: dem TLS Handshake und dem TLS Record. Das Handshake-Protokoll ist für den sicheren Schlüsselaustausch, die Authentifizierung der Kommunikationsteilnehmer und die Aushandlung der kryptographischen Parameter zuständig. Das Record-Protokoll nutzt die ausgehandelten Parameter, um den Datenverkehr zu schützen, sodass dieser nur an den Endpunkten lesbar ist.

Zu den wichtigsten Diensten von TLS gehört die Verschlüsselung, die die übertragenen Daten verbirgt, die Authentifizierung, die die Identität der Endparteien bestätigt, und die Integrität, die sicherstellt, dass die Daten während der Übertragung nicht manipuliert wurden. TLS arbeitet dabei transparent und kann leicht eingesetzt werden, um Protokollen ohne eigene Sicherheitsmechanismen abgesicherte Verbindungen zur Verfügung zu stellen.

Digitale Zertifikate spielen eine entscheidende Rolle bei TLS. Sie werden von einer vertrauenswürdigen Zertifizierungsstelle (CA) ausgestellt und bestätigen die Eigentümerschaft des öffentlichen Schlüssels des Servers. Diese Zertifikate sind auch für die Authentifizierung und die Integrität der Datenübertragung von Bedeutung.

TLS ist universell einsetzbar und wird in nahezu allen Bereichen eingesetzt, in denen Daten übertragen werden, wie beispielsweise im Web (HTTPS), bei E-Mail (SMTP, POP3, IMAP), File Transfer (FTPS) und in der Internet-Telefonie (VoIP).

## Zusammenfassung

TLS ist ein grundlegendes Sicherheitsprotokoll, das die sichere Übertragung von Daten im Internet gewährleistet. Es bietet sowohl Verschlüsselung als auch Authentifizierung und gewährleistet die Integrität der übertragenen Daten. Die neueste Version, TLS 1.3, bietet verbesserte Sicherheit und Effizienz. TLS ist ein wesentlicher Bestandteil der modernen Internetkommunikation und trägt dazu bei, die Privatsphäre und Sicherheit der Nutzer zu schützen.

# Wie funktioniert TLS?

Transport Layer Security (TLS), früher bekannt als Secure Sockets Layer (SSL), ist ein Protokoll, das die sichere Übertragung von Daten über das Internet ermöglicht. Es funktioniert, indem es eine verschlüsselte Verbindung zwischen dem Client (zum Beispiel einem Webbrowser) und dem Server herstellt.

Der Prozess beginnt mit dem sogenannten "Handshake". Der Client sendet eine "Client Hello"-Nachricht an den Server, in der er seine TLS-Version, die unterstützten Verschlüsselungsalgorithmen und eine zufällig generierte Zeichenfolge (Client Random) bekannt gibt. Der Server antwortet mit einer "Server Hello"-Nachricht, in der er die ausgewählten Parameter bestätigt und sein eigenes Zertifikat und eine ebenfalls zufällig generierte Zeichenfolge (Server Random) sendet. Das Zertifikat enthält den öffentlichen Schlüssel des Servers und wird von einer Zertifizierungsstelle (CA) ausgestellt, die die Identität des Servers bestätigt.

Der Client überprüft das Zertifikat des Servers und generiert dann einen sogenannten "Pre-Master-Secret", eine weitere zufällige Zeichenfolge. Dieser Pre-Master-Secret wird mit dem öffentlichen Schlüssel des Servers verschlüsselt und an den Server gesendet. Sowohl der Client als auch der Server verwenden nun den Pre-Master-Secret und die zuvor ausgetauschten Random-Werte, um den Sitzungsschlüssel zu berechnen. Dieser Schlüssel wird für die symmetrische Verschlüsselung der Datenübertragung verwendet.

## Hauptkomponenten und wichtigste Dienste von TLS

Die Hauptkomponenten von TLS sind das Handshake-Protokoll und das Record-Protokoll. Das Handshake-Protokoll ist für den sicheren Austausch des Sitzungsschlüssels und die Authentifizierung der Kommunikationspartner verantwortlich. Das Record-Protokoll verwendet den Sitzungsschlüssel, um die Daten zu verschlüsseln und zu übertragen.

Die wichtigsten Dienste von TLS sind:

1. \*\*Verschlüsselung\*\*: TLS verschlüsselt die Daten, die zwischen dem Client und dem Server übertragen werden, um sie vor unbefugtem Zugriff zu schützen.

2. \*\*Authentifizierung\*\*: Durch den Austausch von Zertifikaten während des Handshakes kann der Client die Identität des Servers überprüfen. Dies schützt vor Man-in-the-Middle-Angriffen.

3. \*\*Integritätsschutz\*\*: TLS stellt sicher, dass die übertragenen Daten während der Übertragung nicht verändert wurden. Dies wird durch den Einsatz von Message Authentication Codes (MACs) erreicht.

Zusammenfassend lässt sich sagen, dass TLS ein wesentliches Protokoll für die sichere Kommunikation im Internet ist. Es ermöglicht die Verschlüsselung von Daten, die Authentifizierung von Kommunikationspartnern und den Schutz der Integrität der übertragenen Daten.