Testat FKOM

Name: Boss

**TLS 1.3 - für ein sicheres Internet**

TLS (Transport Security Layer) ist das vom IEFT entwickelte Sicherheitsprotokoll. Es soll den Verkehr im Internet privat und sicher gestalten. Dies erreicht es mit dem Verbinden von diversen kryptografischen Verfahren. Es soll für die Benutzer ohne zusätzlichen Aufwand benutzbar sein und trotzdem ein Höchstmass an Sicherheit bieten.

Seit einiger Zeit ist Version 1.3 öffentlich verfügbar. Darin sind viele Altlasten aus früheren Zeit entfernt. So sind die Angriffsfläche minimiert und Probleme der alten Versionen mitigiert.

TLS 1.3

Die neue Spezifikation bringt zwei Hauptvorteile: bessere Sicherheit und höhere Geschwindigkeit. Die Sicherheit wird erreicht, in dem viele unsichere Konfigurations-Optionen entfernte wurden.

Dies wäre durch die korrekte Konfiguration schon in Version 1.2 möglich, wird aber häufig nicht gemacht. Dies kann sogar ausgenutzt werden, indem man Verbindungen auf schwache Verschlüsslungen herunterzwingt und somit einfachen Traffic mitlesen kann.

Die verbesserte Geschwindigkeit erreicht die IEFT durch das Vereinfachen des Handshakes.

**TLS-Handshake vor TLS 1.3**

Ähnlich wie TCP kennt TLS ebenfalls einen Handshake. Dieser wird benötigt, um die sichere Kommunikation aufzubauen.

Für das Beispiel verwenden wir Alice als Client und Bob als Server.

Hilfreich ist ein gewisses Verständnis von asymmetrischer Verschlüsselung und Zertifikaten im Internet.

The ‚client hello‘ message: A sendet ein ‘client hello’ an B. Dieser beinhaltets A Verschlüsslungscipher und einen zufälligen Schlüssel, welcher sich A ausgedacht hat.

The ’server hello‘ message: B sendet A die gewählte Verschlüsslungscipher, seinen Public Key und ebenfalls einen zufälligen Schlüssel.

Authentication: A verifiziert den Public Key von B bei der Certificate Authority.

The premaster secret: A sendet verschlüsselt mit dem public Key von B eine Art Challenge.

Private key used: B entschlüsselt die Challenge mit seine private Key.

Session keys created: Durch ein bisschen Mathematikmagie können nun A und B denselben Session Key erzeugen. Weitere Informationen findet man z. B. hier(Diffie-Hellman).

Ready Message: A und B schicken beide verschlüsselt mit dem Session Key ein ‘Ready’.

Session established: Ab hier kommunizieren A und B nur noch verschlüsselt.

TLS-Handshake mit TLS 1.3

The ‚client hello‘ message: A macht eigentlich immer noch dasselbe. Nur sendet es nun bereits mehr Information zum gewünschten Verschlüsslungsverfahren mit. A versucht zu raten, welche Cipher der Server verwenden kann.

The ’server hello‘ message: B schickt die Bestätigung auf die Anfrage von A, Verschlüsslungsinformationen, sein Zertifikat und das ‘Server Ready’. Aus den Informationen generiert er hier bereits den Session Key.

Optional: Falls der B die Verschlüsselung nicht bestätigen kann. Sendet B eine Alternativ zurück, welche A noch einmal bestätigt.

Session established: A kontrolliert das Zertifikat von B, erstellt den Session Key und sendet das ‘Client Ready

\*Falls A beim ersten Schritt etwas Falsches annimmt (Cipher), kann es zu einer zweiten Runde kommen.

tls 1.3 handshake performance

Vergleich von des TLS Handshakes von Version 1.2 zu 1.3. Beim TLS 1.3 ist zu beachten, dass die ein Full-Handshake ist. Dies passiert, falls beim Schritt 1 eine falsche Annahme getroffen wurde. (Bei Grafik Quelle angeben)

Weitere wurde mit 1.3 das Feature 0-RTT Resumption implementiert. Dieses speicher die Kommunikatiosinformationen zwischen Client und Server. Diese können wiederverwendet werden, falls notwendig.

Dieses Feature ist umstritten, weil es Replay Attacks und ähnliche Probleme mitbringt. Wenn jemand diese Informationen auslesen kann, könnten weitere Kommunikationen eventuell mitgeschnitten oder intercepted werden.

Auswirkung auf den Endnutzer

Der Endnutzer wird nichts grossartiges bemerken. Auch wenn die Geschwindigkeit im Internet wichtig ist, ist dies eher spannend für die Serverbetreiber. Diese verarbeiten Millionen von solchen Verbindung und somit machen 1-2 Milisekunden einen grossen Unterschied.

Interessant ist hier eher der Sicherheitsaspekt, wobei auch hier viele den Unterschied nie bemerken werden.

Auswirkung für Firmen

Wie erwähnt ist die Performance-Verbesserung für Serverbetreiber spannend, da die Zeit für einen Verbindungsaufbau praktisch halbiert wurde.

Es gab Befürchtungen, dass TLS 1.3 SSL Inspection verhindert; daher wurde eine Backdoor verlangt. Dies wurde aber offiziell abgelehnt und nicht in die Spezifikation aufgenommen. Wenn jemand die öffentlichen E-Mails liest, wird nicht klar, woher die Angst vor TLS 1.3 kommt.

Quellen

Transport Layer Security

https://en.wikipedia.org/wiki/Transport\_Layer\_Security

HTTPS

https://en.wikipedia.org/wiki/HTTPS

What Is Transport Layer Security (TLS)?

https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/

TLS 1.3: What This Means For You (Alex Samonte, 15.04. 2019)

https://www.fortinet.com/blog/business-and-technology/tls-is-here-what-this-means-for-you.html

TLS 1.3 Handshake: Taking a Closer Look (Jay Thakkar, 20.04.2018)

https://www.thesslstore.com/blog/tls-1-3-handshake-tls-1-2/

[TLS] Industry Concerns about TLS 1.3

http://hslu.blz.ch/fkom/wordpress/?post\_type=wpws\_content&p=278&preview=true

# Beurteilungsraster für den Blogbeitrag

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Informationsgehalt, Relevanz, Aktualität | 5 |  |  |  |  |  |  |
| Strukturierung, Titel, Lead |  |  | 3 |  |  |  | * Beispiel ist zu langatmit; einen separaten Kasten machen * Guter Titel und gutes Lead |
| Vernetzung, intern / extern | 5 |  |  |  |  |  |  |
| Stilistik,  Zielgruppe |  |  | 3 |  |  |  | * Gross-/Kleinschreibung beachten * Artikel setzen; Syntax beachten * Fachbegriffe möglichst vermeiden |
| Korrektheit, Quellenangabe | 5 |  |  |  |  |  | * Apa; aber das konnten Sie damals noch nicht wissen. |
| Punkte TOTAL | 21 | | | | | | Maximum: 25 Punkte |

Testat bestanden; gute Arbeit