NWES
5AHWII
Alexander Heim, Niklas Schneider

HTTPS und TLS

HTTPS steht für "**H**yper**t**ext **T**ransfer **P**rotocol **S**ecure". Es ist eine Erweiterung des Internetprotokolls HTTP, welches die Kommunikationsvorgänge im World Wide Web mittels Hypertext Dokumenten (Webseiten) und Hyperlinks definiert. Im Gegensatz zu HTTP versucht HTTPS die Sicherheit der Kommunikation zu gewährleisten. Das Problem bei HTTP ist, dass alle gesendeten Daten lesbar sind. Jeder könnte den Datenverkehr mitlesen und wichtige Informationen extrahieren. Um dieses Problem zu lösen, wurde HTTPS erschaffen. HTTPS, heutzutage auch bekannt als HTTP over TLS, setzt dabei auf das kryptografische Protokoll TLS, welches unter anderem auch bei Emails und Voice-over-IP Gebrauch findet. Früher wurde der Vorgänger von TLS namens SSL verwendet. Dieser wurde aber durch TLS ersetzt, da SSL unter einigen Sicherheitslücken leidet.

TLS

Auch TLS wird ständig weiterentwickelt. Die momentan aktuellste Version lautet TLS 1.3 und wurde 2018 veröffentlicht. Das primäre Ziel von TLS ist die Bereitstellung eines sicheren Kommunikationskanals zwischen zwei Geräten. Der Kanal muss folgende Aufgaben erledigen, um als sicher zu gelten:

- **Authentifizierung:**
  Die Serverseite des Kommunikationskanals ist immer authentifiziert. Die Echtheit und Übereinstimmung der tatsächliche Identität des Servers ist somit sichergestellt. Die Authentifizierung des Clients ist optional.
  Die Authentifizierung kann mittels asymmetrischer Kryptografieverfahren (RSA, ECDSA, EdDSA) oder mittels eines symmetrischen pre-shared keys (PSK) realisiert werden.

- **Geheimhaltung/Verschlüsselung:**
  Über den Kommunikationskanal gesendete Daten sind nur für Sender und Empfänger lesbar.
  Zwischengeschaltete Maschinen sind nicht in der Lage, die gesendeten Daten mitzulesen.
  Die Länge der Nachricht wird dabei standardmäßig nicht geheim gehalten.

- **Sicherstellung der Datenintegrität:**
  Daten, welche über den Kommunikationskanal gesendet werden, können nicht unbemerkt von Zwischenmännern verändert werden.

Diese Eigenschaften sollten auch in einem von einem Angreifer völlig kontrollierten Netzwerk bestehen.

Ablauf von TLS:

TLS besteht aus zwei primären Teilen, um eine sichere Verbindung aufzubauen und zu gewährleisten:

1. **Handshake:**
   In dieser Phase wird Sender und Empfänger authentifiziert und kryptografische Parameter ausgehandelt. Das Handshake-Protokoll ist so entworfen, dass es gegen Manipulation eines Angreifers resistent ist. Der Handshake regelt also folgende Dinge:
   a. Die Geräte einigen sich auf die zu verwendende TLS Version

   b. Die Geräte einigen sich auf die zu verwendenden Verschlüsselungsverfahren
   c. Die Serveridentität wird mit einem TLS-Zertifikat überprüft
   d. Die Sitzungsschlüssel für die Verschlüsselung der Daten werden generiert

2. **Record:**
   Nutzt die beim Handshake ausgehandelten Parameter um einen sicheren Datenverkehr zu ermöglichen. Das Record Protokoll unterteilt die gesendeten Nachrichten in eine Reihe von Datensätze ein, welche eigenständig gesichert und unkenntlich gemacht werden.

SSl/TLS-Zertifikate

Da HTTPS auf TLS basiert, muss auch beim Verwenden vom HTTPS-Protokoll eine TLS Verbindung aufgebaut werden.

Um die Identität des Servers zu überprüfen, finden beim Handshake digitale Zertifikate Verwendung. Dieser Handshake sieht im World Wide Web folgendermaßen aus:

1. Ein Browser versucht eine Verbindung über TLS mit einer Website (Server) aufzubauen (Client und Server Hello).
2. Der Browser bittet den Server, sich zu identifizieren.
3. Der Server sendet dem Webbrowser eine Kopie seines X.509-Zertifikates als Antwort.
4. Der Browser entscheidet, ob er dem Zertifikat traut. Bei Vertrauen in das Zertifikat sendet der Browser dem Server ein Signal.
5. Der Server startet dann die TLS-verschlüsselte Verbindung.
6. Die Verbindung ist nun aufgebaut und sichergestellt.

Will man einem Server ermöglichen, eine HTTPS Verbindung mit den Clients aufzubauen, muss man dem Server natürlich ein Zertifikat geben. Zertifikate werden von Certificate Authorities (CA) ausgeben. Üblicherweise ist die Zertifikatausstellung mit Kosten verbunden.

Der Browser validiert das erhaltene Zertifikat mit dem „Online Certificate Status Protocol“. Dabei fragt er die verantwortliche Zertifizierungsstelle an, ob das Zertifikat gültig ist. Ein Problem: Bekommt der Browser keine Antwort vom Zertifikataussteller, muss er selbst entscheiden, ob er das Zertifikat als sicher ansieht.

SSL/TLS-Zertifikate sind nicht ewig gültig. Sie besitzen ein Ablaufdatum. Das Certificate Authority/Browser Forum hat verkündigt, dass Zertifikate eine maximale Lebensdauer von 27 Monaten nicht überschreiten sollten. Der Sinn darin ist, dass die Zertifikatinhaber regelmäßig von den Ausstellern geprüft werden müssen.

Benutze ich HTTPS?

Um beim Surfen des Internets auf einen schnellen Blick zu überprüfen, ob man eine sichere Verbindung zu einer Website hat (mittels HTTPS), muss man in der Adresszeile eines Browsers (dort wo die URLs und die Standardsuchleiste residieren) schauen. Der Protokollteil in der Adresszeile muss die Buchstaben „https“ beinhalten. Links davon sollte sich das Symbol eines geschlossenen Vorhängeschlosses befinden.

Quellen:

https://www.elektronik-kompendium.de/sites/net/1811281.htm

https://tools.ietf.org/search/rfc2818#section-2.1

https://datatracker.ietf.org/doc/html/rfc8446#section-4.2.4

https://en.wikipedia.org/wiki/X.509

https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate