



50 Jahre Internet – Internetworking 2019 **Abgesicherter Datentransport auf der Transportschicht**

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut
Universität Potsdam

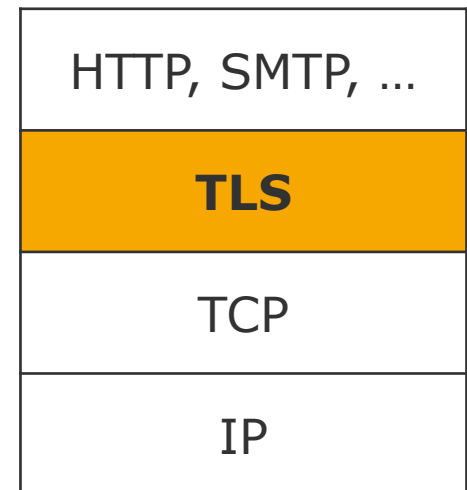
Um gezielt Schutzmaßnahmen ergreifen zu können, müssen die umzusetzenden Sicherheitsziele ermittelt werden.

- Zu den grundlegenden Sicherheitszielen gehören:
 - Verfügbarkeit
 - Datenintegrität
 - Vertraulichkeit
 - Authentifikation
 - Autorisation
 - ...

Um Sicherheitsziele und -anforderungen für Internetanwendungen zu gewährleisten, braucht es geeignete Sicherheitsarchitekturen

- **Absicherung der Protokolle** des TCP/IP-Protokollstapels – also die Bereitstellung von Sicherheitsmechanismen zur Gewährleistung von Sicherheitsziele kann auf unterschiedlichen Schichten erfolgen, z.B. auf der Transportschicht
- Geschickter Einsatz von Sicherheitsmechanismen auf der Transportschicht erübrigt
 - Absicherung der vielen Protokolle auf der Anwendungsschicht
 - aufwändig Absicherung auf Internetschicht

→ **TLS-Protokoll**



SSL – Secure Socket Layer

Zum vertraulichen Datentransport über das WWW entwickelte Netscape 1994 eine eigene sichere Transportinfrastruktur:

- HTTP über SSL – **HTTPS** (mehr zu HTTPS in Woche 6)
- **Idee:** Mit **SSL – Secure Socket Layer** – wird zwischen Anwendungsschicht (z.B. HTTP) und Transportschicht (z.B. TCP) zusätzliche Protokollschicht zur Sicherstellung eines vertraulichen Transports im TCP/IP-Protokollstapel integriert
- Auch andere Protokolle der Anwendungsschicht des TCP/IP-Stacks können ohne weitere Anpassungen die durch SSL bereitgestellten sicheren Verbindungen nutzen, z.B. Online-Banking, E-Shopping, ...
- SSL wurde in der Version 3.0 von der IETF als **TLS – Transport Layer Security** standardisiert. Sprechen darum im Folgenden von **TLS**.

TLS – Transport Layer Security wird nicht nur zur Absicherung von HTTP (WWW) benutzt, sondern auch zur Absicherung von E-Mail-Verbindungen (IMAP+TLS, SMTP+TLS), z.B. bei GoogleMail

TLS bietet Kommunikationspartnern:

- **Private Verbindung** – nach anfänglichem Handshake-Verfahren zum sicheren Schlüsselaustausch für Verschlüsselung werden Daten (symmetrisch) verschlüsselt
- **Authentifikation** über (asymmetrische) Verschlüsselungsverfahren
- **Zuverlässige Verbindung** – überprüft beim Nachrichtentransport Unversehrtheit der transportierten Daten

TLS – Transport Layer Security

TLS im TCP/IP-Schichtenmodell:

