Internet-Transport Absicherung

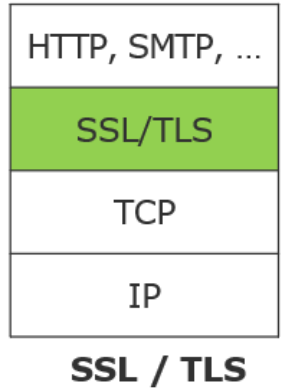
STUDIEREN AUF HÖCHSTEM NIVEAU

Prof. Dr. Jürgen Anders, Hochschule Furtwangen
Fakultät Digitale Medien

Absicherung auf der Transportschicht

Um bestimmte Sicherheitsziele und –anforderungen für verschiedene Internetanwendungen zu erreichen braucht es geeignete Sicherheitsarchitekturen

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



-> SSL/TLS Protokolle

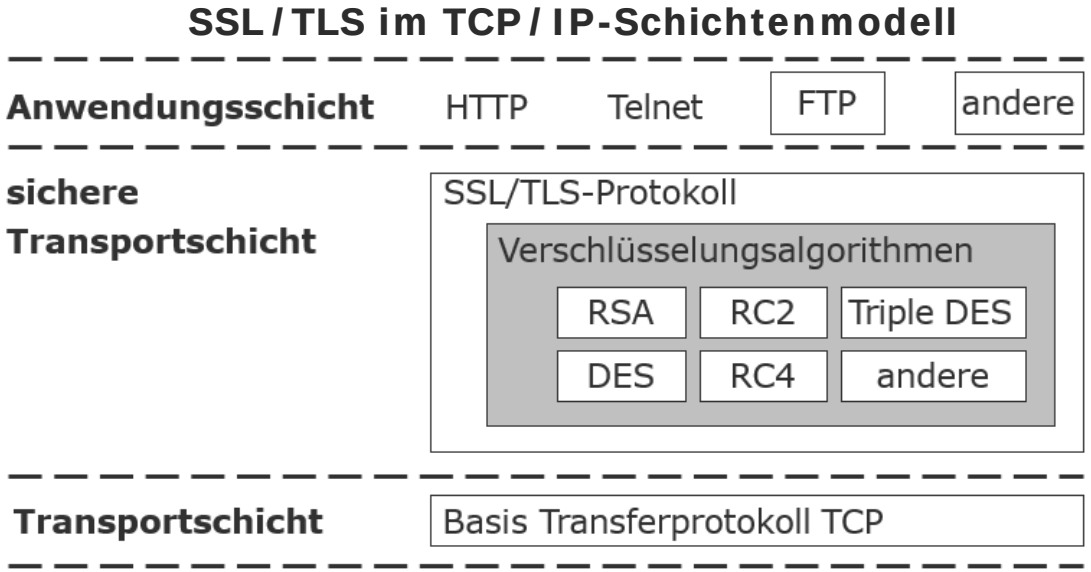
Zum vertraulichen Datentransport über das WWW entwickelte Netscape 1994 eine eigene sichere Transportinfrastruktur:

- HTTP über SSL – HTTPS

- Idee: Mit SSL – Secure Socket Layer – wird zwischen Anwendungsschicht (HTTP) und Transportschicht (TCP) eine neue Protokollschicht zum vertraulichen Transport im TCP/IP-Protokollstapel integriert
- Auch andere Protokolle der Anwendungsschicht des TCP/IP- Protokollstapels 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 IETF als TLS – Transport Layer Security standardisiert. Sprechen darum im Folgenden von SSL/TLS

SSL/TLS bietet Kommunikationspartnern:

- Private Verbindung – nach anfänglichem Handshake-Verfahren zum sicheren Schlüsselaustausch werden Daten symmetrisch verschlüsselt
- Authentifikation über asymmetrische Verschlüsselungsverfahren
- Zuverlässige Verbindung – Nachrichtentransport überprüft Unversehrtheit der transportierten Daten über Message Authentication Code – MAC



Internet-Transport Absicherung

STUDIEREN AUF HÖCHSTEM NIVEAU

Prof. Dr. Jürgen Anders, Hochschule Furtwangen
Fakultät Digitale Medien