Verschlüsselte E-Mail-Kommunikation unter Linux

Florian Knodt <adlerweb@adlerweb.info>

CC BY SA

Warum Verschlüsseln?

- Unverschlüsselte Verbindungen können von vielen Stellen abgefangen und manipuliert werden
  - Internetprovider, Netzbetreiber
  - Geheimdienste
    - Automatische Auswertung?
      - Der PC hat immer recht
  - Benutzer im selben Netzwerk
    - Ich könnte in der Nähe sein ;)

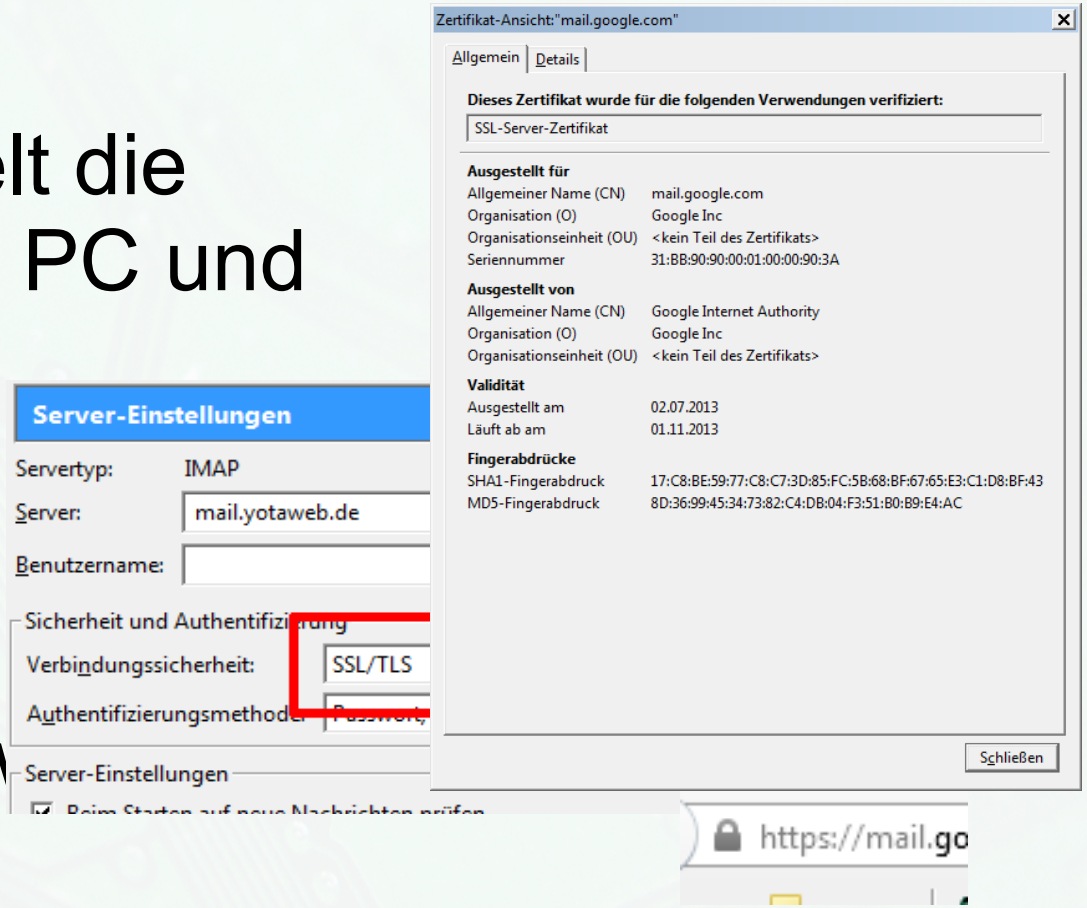
CC BY SA

Demo: Mails mitlesen per Wireshark

CC BY SA

SSL/TLS Benutzen!

- SSL/TLS verschlüsselt die Verbindung zwischen PC und Server
- Inhalt und Metadaten
- Zertifikat prüfen
- Zwischen/am Server v
  unverschlüsselt



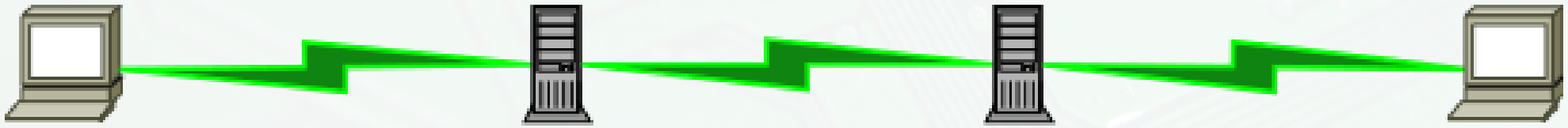
CC BY SA

Demo: Mails am Server abfangen

CC BY SA

Inhaltsverschlüsselung

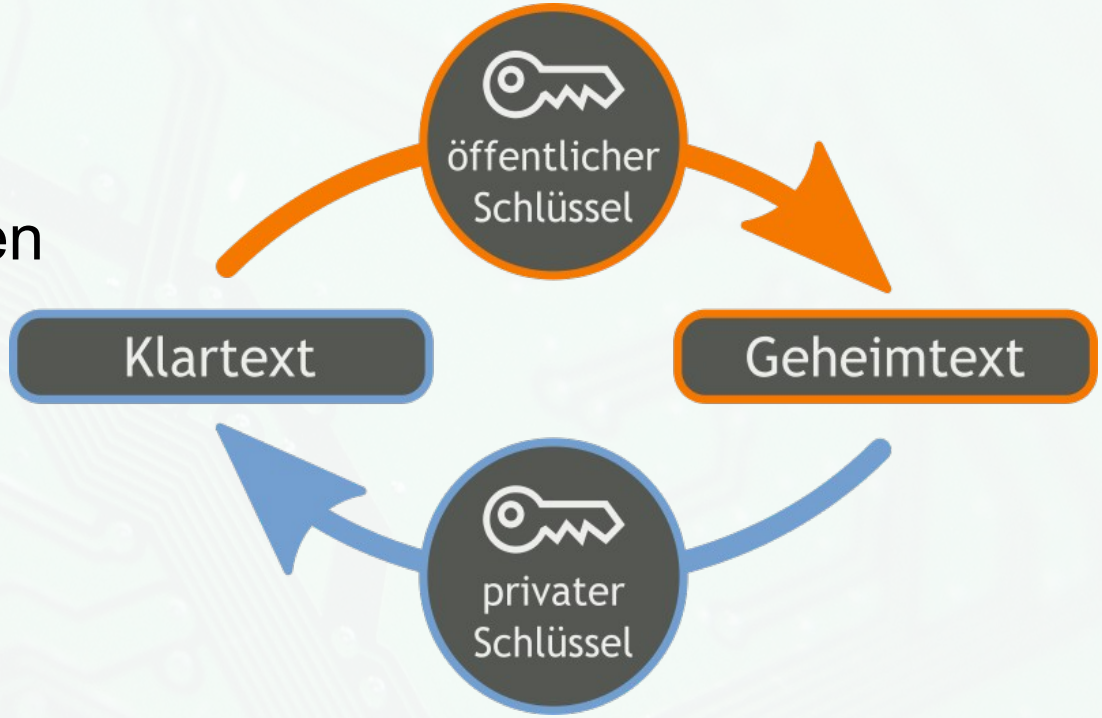
- Mailinhalt wird zwischen den Kommunikationspartnern verschlüsselt
- Sender und Empfänger müssen sich bereits kennen
  - Keyserver lockern diese Einschränkung



CC BY SA

Asymmetrische Kryptografie

- Nicht wie bei symmetrischen Verfahren ein Passwort
- Schlüssel besteht aus 2 Teilen
  - Öffentlicher Schlüssel: Nur verschlüsseln
  - Privater Schlüssel: Nur entschlüsseln



CC BY SA

Standard 1: S/MIME

- Auf X.509 aufbauend
  - Hirarchische Struktur; Zentrale Zertifizierungsstellen
  - Freie Anbieter haben nur wenig Prüfung
  - Gute Prüfung gegen Geld
- Wird von fast allen Mailclients direkt unterstützt
- z.T. auch als Browser-Plugin für Webmail

CC BY SA

Standard 2: PGP

- Basiert auf einem dezentralen WOT
  - Vertrauen muss „erarbeitet“ werden
- Freie Implementierung: GnuPG / GPG
- Für die meisten Mailsysteme als Plugin verfügbar
- Für Firefox und Chrome als Plugin verfügbar
- GPG ist nicht auf E-Mail beschränkt

CC BY SA

Demo: PGP mit Thunderbird und Enigmail

CC BY SA

Demo: PGP im Browser

CC BY SA

Was bleibt

- Inhalt Ende-zu-Ende verschlüsselt
- Metadaten nur teilweise verschlüsselt
  - ~~Vorratsdatenspeicherung~~ Mindestspeicherfrist greift weiterhin!

CC BY SA

...und der Rest?

- Webseiten
  - HTTPS nutzen
  - Tor & Co kann bedingt anonymisieren
- Chat
  - z.B. Pidgin mit OTR, Xabber oder Gibberbot auf Android
- Social Media
  - Dezentralen Systemen wie statusNET und Diaspora die Daumen drücken

CC BY SA

Fragen?

- ...werden auch verschlüsselt entgegen genommen:

  f.knodt@yotaweb.de GPG 0x3DF6966D

CC BY SA