Working principle, attacks and defenses of SSL/TLS

Tom Petersen

University of Hamburg
Department of Informatics

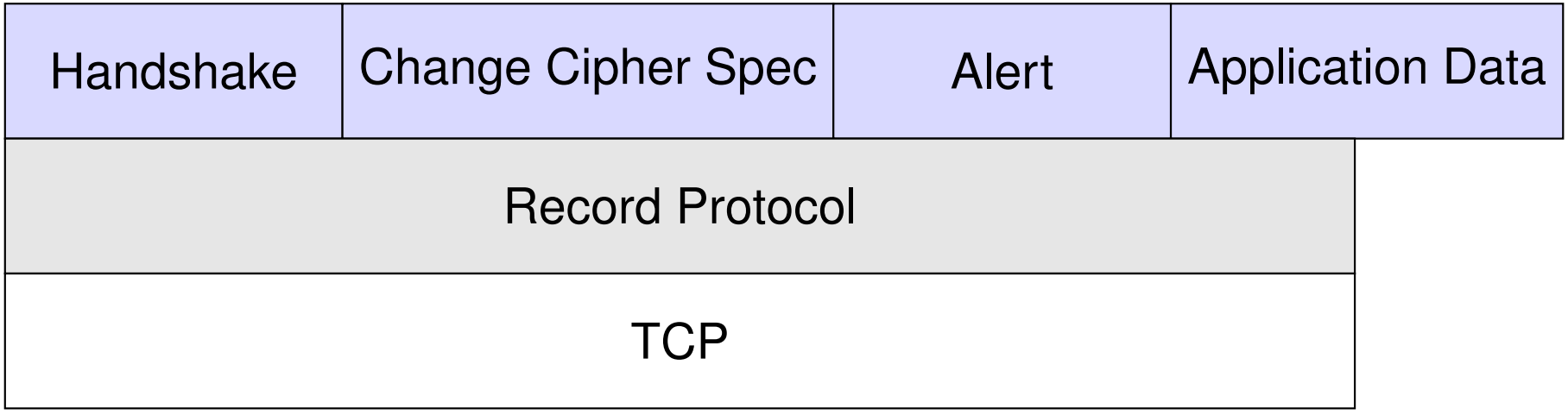
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Agenda

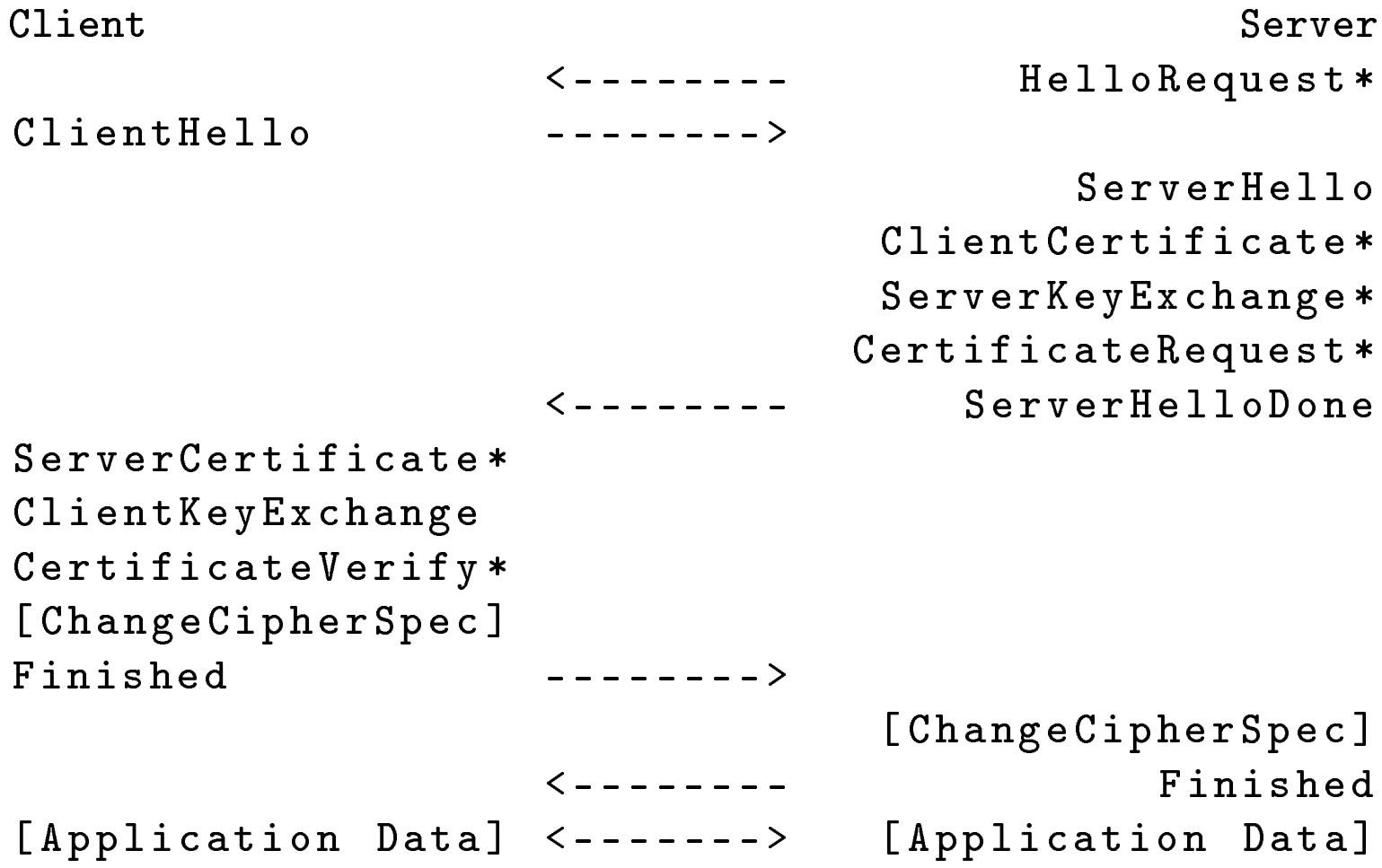
1. Transport Layer Security
2. University teaching
3. Simulating protocols
4. Der Arbeitsbereich SVS
   - Mission
   - Themen
   - Kontakt
5. Beispiel für eine Abbildung
   - Zugangskontrolle
   - DRM-Systeme
6. Weiteres Beispiel für eine Abbildung
7. Ebenen
8. Spalten

- authentication of communication partners, encryption and integrity check of sent messages
- widely used in HTTPS, SFTP, SMTPS, ...
- developed as a part of netscape navigator in the early 90s (1994) as SSL (v1, v2, v3) and was soon used in other browsers and applications
- 1999 IETF standardized it as TLS 1.0
- current 1.2, 1.3 in progress

Protocol hierarchie



Message flow



- brief overview (usage, historical version history) - working principle
- message overview image from RFC, subprotocols - key material - cipher suites
- reasons for using TLS in university teaching - fundamental ideas/ didactic reduction

- advantages of using exploration/simulations in teaching -> protocol.edu - TLS plugin - extensions/plugins

Der Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

Lorem ipsum dolor

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

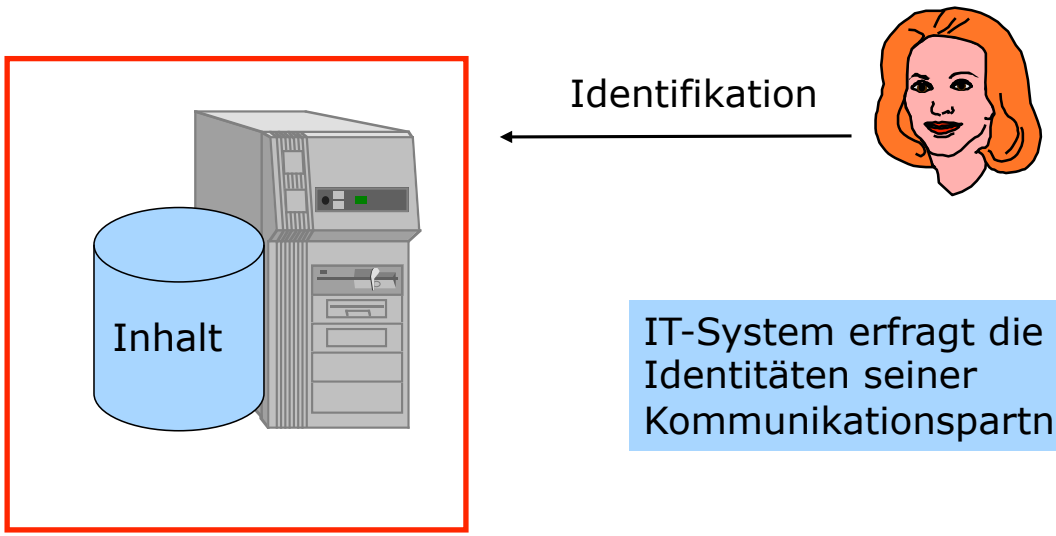
- Themen
  1. Privacy Enhancing Technologies (PET)
  2. Security Management & Risk Management
  3. Security of Mobile Systems
- Weitere Informationen
  - http://www.informatik.uni-hamburg.de/svs

Beispiel für eine Abbildung

- Zweck
  - Nur mit berechtigten Partnern weiter kommunizieren
  - Verhindert unbefugte Inanspruchnahme von Betriebsmitteln

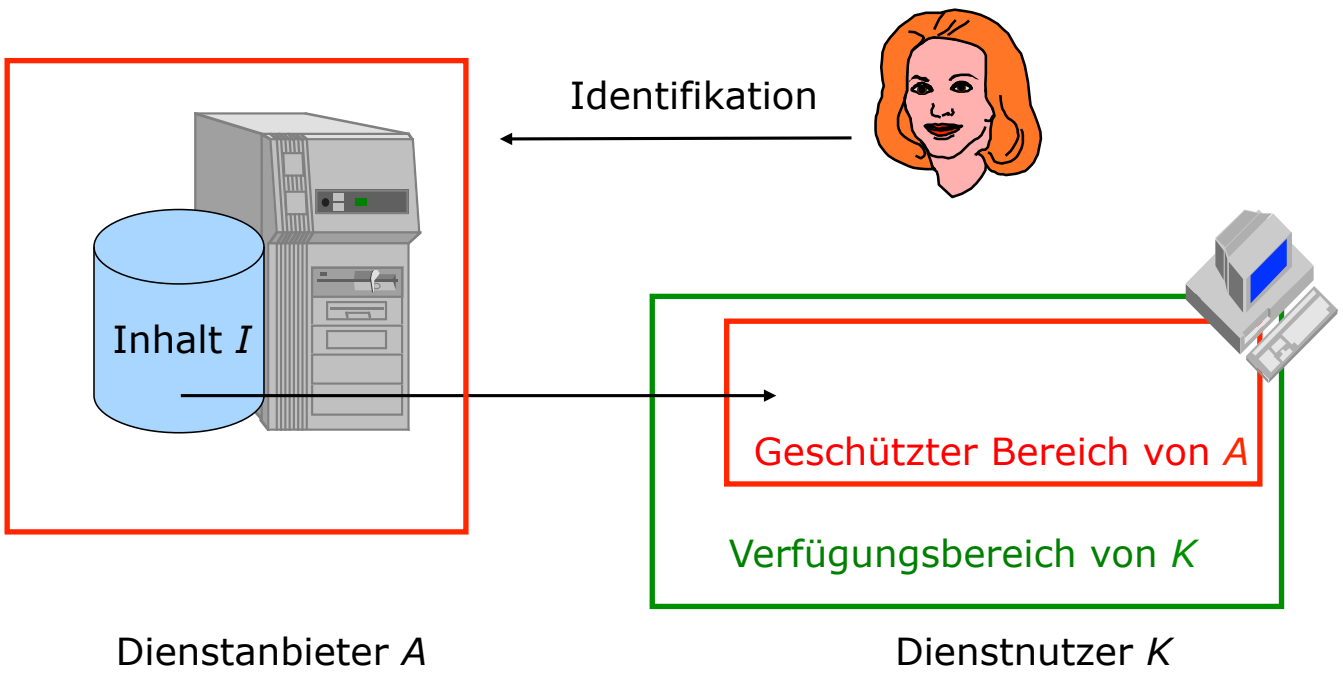
Beispiel für eine Abbildung

- Zweck
  - Nur mit berechtigten Partnern weiter kommunizieren
  - Verhindert unbefugte Inanspruchnahme von Betriebsmitteln



Beispiel für eine Abbildung

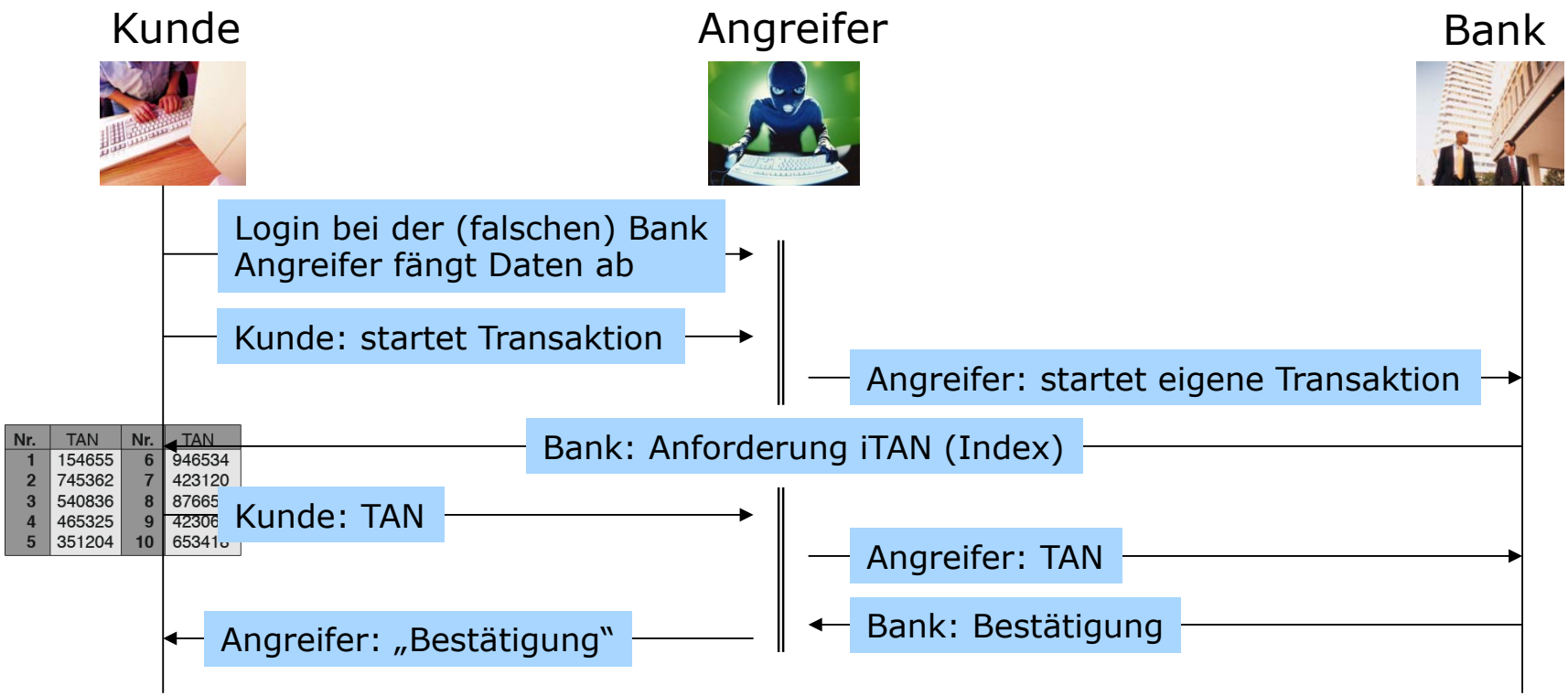
- Zweck
  - Einem Kunden *K* einen Inhalt *I* in einer bestimmten Weise zugänglich machen, ihn aber daran hindern, *alles* damit tun zu können.



Weiteres Beispiel für eine Abbildung

[John Doe, 1966]

- Voraussetzung: Angreifer
  - betreibt täuschend echte Webseite der Bank
  - bewegt den Kunden zum Besuch dieser Seite



Ebenen

- Erste Ebene
  - Zweite Ebene
    - Dritte Ebene
  - Zweite Ebene
- Erste Ebene

1. Erste Ebene
   1.1 Zweite Ebene
      1.1.1 Dritte Ebene
   1.2 Zweite Ebene
2. Erste Ebene

Spalten

- Linke Spalte
  - Lorem ipsum dolor sit amet,
  - consectetur adipisicing elit,
  - sed do eiusmod tempor incididunt ut
  - labore et dolore magna aliqua.
- Erste Ebene
  - Zweite Ebene
  - Zweite Ebene
- Erste Ebene
  - Zweite Ebene
  - Zweite Ebene

Das SVS-Logo