



# 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

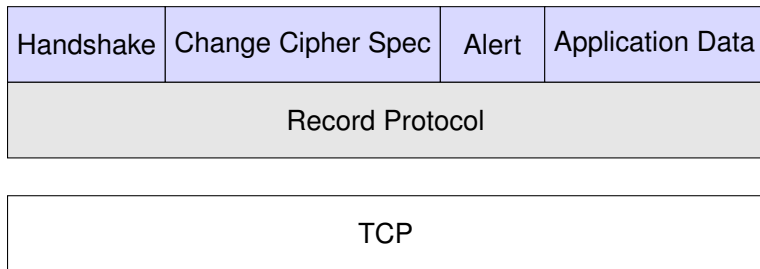
3. Simulating protocols

## TLS Overview

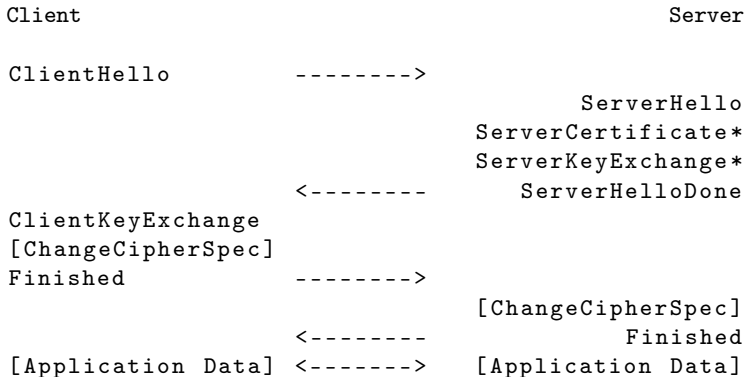
---

- 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



*Based on the TLS 1.2 specification, RFC 5246.*

## Cipher suites

---

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

## Didactic reduction (?)

---

- concrete methods (like protocols) should be abstracted
- long-lasting principles, which are used in multiple fields
  - hybrid cryptosystems
  - authenticated key exchange
  - side-channel attacks
  - cryptographic principles

## Explorative learning

---

- discovering and studying a topic by oneself
- useful for complex topics, which are hard to understand with other learning materials
- requires appropriate software: often simulations are used =  
interactive computer programs modelling activities, which enable us  
to observe normally hidden processes



## Developed application

---

- application for simulating two party protocol flows
- TLS plugin

## Live demo

---

- cipher suite choosing
- server/client views
- start connection
- updated values in tree view
- message and message details view
- info view
- finish handshake
- edit bytes and watch occurring error
- echo plugin (?)

## Possible extensions

---

- extendable (requirement)
- not implemented in TLS plugin (?) p. 39
  - TLS extensions
  - client authentication
  - session resuming
  - certificate validation

## Conclusion

---

whatever, maybe previous slide as part of the conclusion?