



# Working principle, attacks and defenses of SSL/TLS

Tom Petersen

University of Hamburg  
Department of Informatics



Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

# TLS

---

- security protocol above the transport layer
- authentication of communication partner(s)
- encryption and integrity check
- used by many higher layer protocols and applications

---

<sup>1</sup>[Jörg Schwenk. Sicherheit und Kryptographie im Internet. 4. Auflage Springer Vieweg, 2014.

# TLS

---

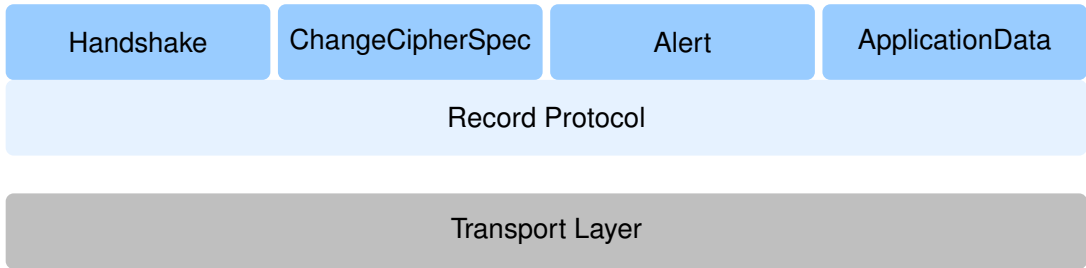
- security protocol above the transport layer
- authentication of communication partner(s)
- encryption and integrity check
- used by many higher layer protocols and applications
- SSL/TLS is the most used security protocol today. <sup>1</sup>
- many attacks and countermeasures
- easy specification

---

<sup>1</sup>[Jörg Schwenk. Sicherheit und Kryptographie im Internet. 4. Auflage Springer Vieweg, 2014.

## Protocol hierarchie

---



# Fundamental ideas

## Fundamental ideas

long-lasting principles, which are applicable or observable in multiple contexts.

Andreas Schwill. Computer Science Education based on Fundamental Ideas. <http://ddi.uni-muenster.de/didaktik/Forschung/Israel97.pdf> (Retrieved 07.1.2016)

Examples:

# Fundamental ideas

## Fundamental ideas

long-lasting principles, which are applicable or observable in multiple contexts.

Andreas Schwill. Computer Science Education based on Fundamental Ideas. <http://ddi.uni-muenster.de/didaktik/Forschung/Israel97.pdf> (Retrieved 07.1.2016)

Examples:

- hybrid cryptosystems

# Fundamental ideas

## Fundamental ideas

long-lasting principles, which are applicable or observable in multiple contexts.

Andreas Schwill. Computer Science Education based on Fundamental Ideas. <http://ddi.uni-muenster.de/didaktik/Forschung/Israel97.pdf> (Retrieved 07.1.2016)

Examples:

- hybrid cryptosystems
- authenticated key exchange

# Fundamental ideas

## Fundamental ideas

long-lasting principles, which are applicable or observable in multiple contexts.

Andreas Schwill. Computer Science Education based on Fundamental Ideas. <http://ddi.uni-muenster.de/didaktik/Forschung/Israel97.pdf> (Retrieved 07.1.2016)

Examples:

- hybrid cryptosystems
- authenticated key exchange
- side-channel attacks



# Fundamental ideas

## Fundamental ideas

long-lasting principles, which are applicable or observable in multiple contexts.

Andreas Schwill. Computer Science Education based on Fundamental Ideas. <http://ddi.uni-muenster.de/didaktik/Forschung/Israel97.pdf> (Retrieved 07.1.2016)

Examples:

- hybrid cryptosystems
- authenticated key exchange
- side-channel attacks
- cryptographic principles, e.g. unpredictable IVs

## Discovery learning and simulations

---

### **Discovery learning** (also **exploratory learning**)

learning by interacting with the world by exploring and manipulating objects and performing experiments.

J. S. Bruner. On Knowing: Essays for the left hand. Harvard University press, 1979.

## Discovery learning and simulations

### **Discovery learning** (also **exploratory learning**)

learning by interacting with the world by exploring and manipulating objects and performing experiments.

J. S. Bruner. On Knowing: Essays for the left hand. Harvard University press, 1979.

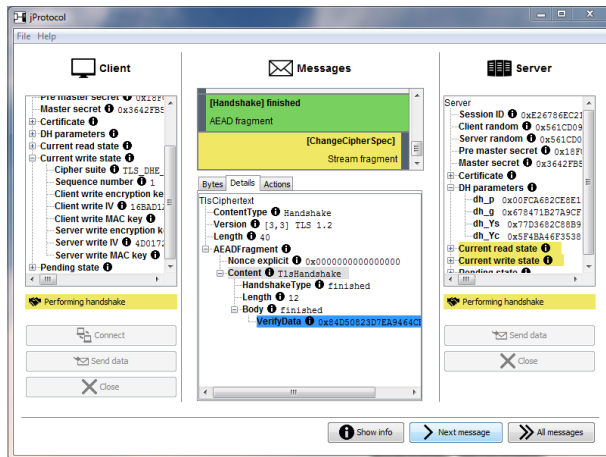
### **Simulations**

interactive computer programs modelling activities, which enable us to observe normally hidden processes.

Helmut M. Niegemann et al. Kompendium multimediales Lernen. Springer, 2008.

# Live demo

- Simulating TLS
- Observable message flow
- Extendable



The screenshot displays the jProtocol application interface, which is divided into three main panels: Client, Messages, and Server.

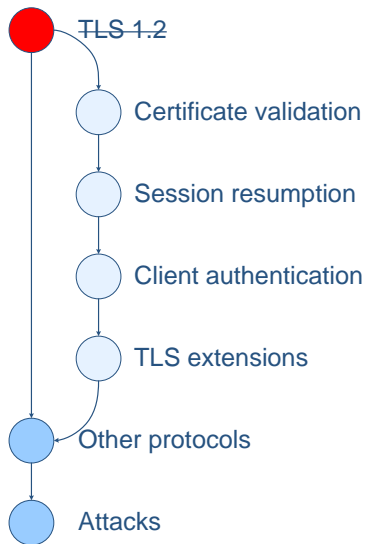
- Client Panel:** Shows the state of the client during the handshake. The "Pending state" is selected, indicating the handshake is in progress. A yellow bar at the bottom indicates "Performing handshake". Buttons for "Connect", "Send data", and "Close" are visible.
- Messages Panel:** Displays the message flow. The "Handshake" message is highlighted in green, and the "AEAD fragment" is highlighted in yellow. The "Stream fragment" is also visible. The "Details" tab is active, showing the structure of the TLS handshake message, including the "Content" (HandshakeType) and "Body" (VerifyData).
- Server Panel:** Shows the state of the server. The "Current read state" and "Current write state" are highlighted in yellow. A yellow bar at the bottom indicates "Performing handshake". Buttons for "Send data" and "Close" are visible.

The "Details" tab in the Messages panel shows the following structure for the TLS handshake message:

```

    TlsCiphertext
    - ContentType: Handshake
    - Version: [3,3] TLS 1.2
    - Length: 40
    - AEADFragment
      - Nonce explicit: 0x0000000000000000
      - Content: TlsHandshake
        - HandshakeType: finished
        - Length: 12
        - Body: finished
          - VerifyData: 0x84D50B23D7EA9464CF
  
```

## Possible next steps



---

Thank you!