



Working principle, attacks and defenses of SSL/TLS

Tom Petersen

University of Hamburg
Department of Informatics



Universität Hamburg

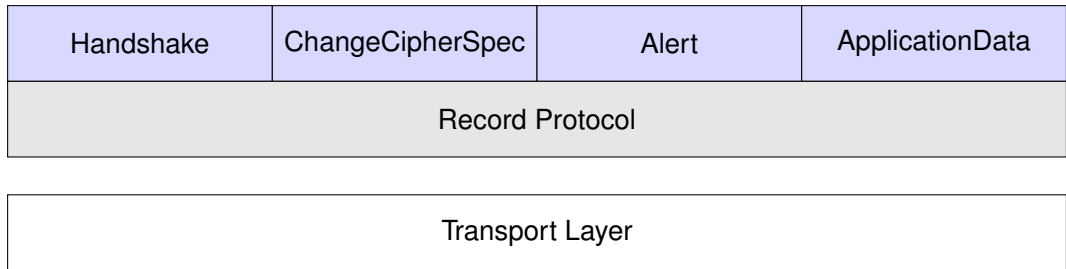
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Motivation TLS

- security protocol above the transport layer of the OSI model
- provides authentication of communication partners, encryption and integrity check of sent messages
- used by many higher layer protocols and applications
- SSL/TLS is the most used security protocol today. ¹

¹[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 with 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

The screenshot displays the iProtocol application window, which is divided into three main panels: Client, Messages, and Server. The Client panel on the left shows the state of the client during a TLS handshake, including fields like Pre master secret, Master secret, Certificate, DH parameters, and various encryption keys. The Messages panel in the center shows the sequence of messages exchanged, with a green bar for "[Handshake] finished" and a yellow bar for "[ChangeCipherSpec]". The Server panel on the right shows the state of the server, including Session ID, Client random, Server random, Pre master secret, Master secret, Certificate, and DH parameters. The bottom of the window features buttons for "Performing handshake", "Connect", "Send data", "Close", "Show info", "Next message", and "All messages".

Client

- Pre master secret 0x18F1
- Master secret 0x3642FB8
- Certificate
- DH parameters
- Current read state
- Current write state
- Cipher suite TLS_DHE
- Sequence number 1
- Client write encryption key
- Client write IV 16BAD1
- Client write MAC key
- Server write encryption key
- Server write IV 4D017
- Server write MAC key
- Pending state
- Performing handshake
- Connect
- Send data
- Close

Messages

- [Handshake] finished
- AEAD fragment
- [ChangeCipherSpec]
- Stream fragment
- TlsCipherText
 - ContentType Handshake
 - Version [3,3] TLS 1.2
 - Length 40
 - AEADFragment
 - Nonce explicit 0x0000000000000000
 - Content TlsHandshake
 - HandshakeType finished
 - Length 12
 - Body finished
 - VerifyData 0x84D50823D7EA944C

Server

- Session ID 0xE26786EC21
- Client random 0x561CD09
- Server random 0x561CD0
- Pre master secret 0x18F1
- Master secret 0x3642FB8
- Certificate
- DH parameters
 - dh_p 0x00FCA682CE8E1
 - dh_g 0x678471B27A9CF
 - dh_Ys 0x77D3682C88B9
 - dh_Yc 0x5F4BA46F3538
- Current read state
- Current write state
- Pending state
- Performing handshake
- Send data
- Close

Possible next steps

- Unimplemented in TLS plugin
 - certificate validation
 - session resumption
 - client authentication
 - TLS extensions
- Implement other protocols

Thank you!