



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

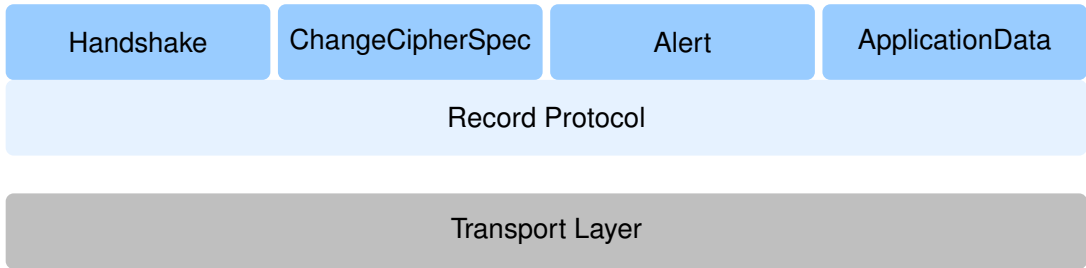
¹[Jörg Schwenk. Sicherheit und Kryptographie im Internet. 4. Auflage Springer Vieweg, 2014.

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. ¹
- many attacks and countermeasures
- easy specification

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

Protocol Hierarchy



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.

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.

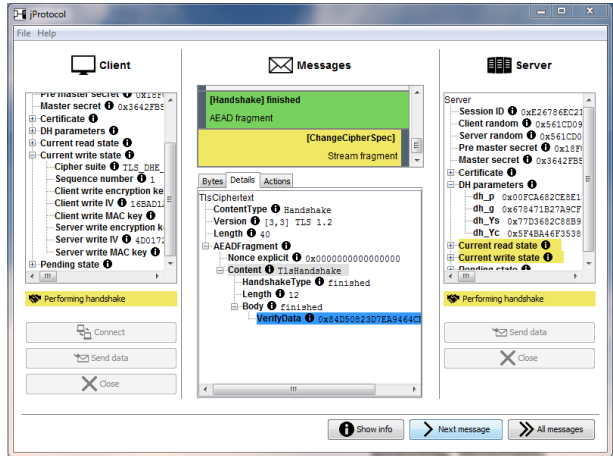
Simulations

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

- Simulating TLS
- Observable message flow
- Extendable

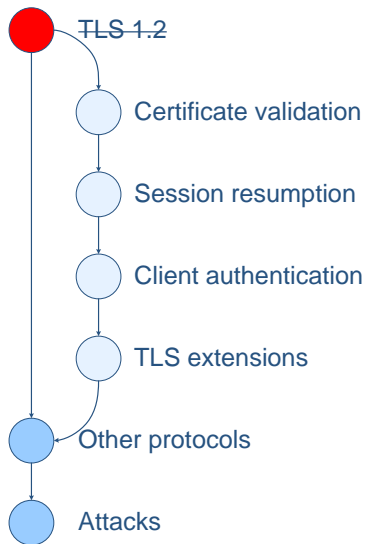


The screenshot displays the jProtocol application interface, which is divided into three main panels: Client, Messages, and Server.

- Client Panel:** Shows the state of the client during the handshake. The "Pending state" is selected, and the "Performing handshake" button is highlighted. The state list includes: Pre master secret, Master secret (0x3642FB5), Certificate, DH parameters, Current read state, Current write state, Cipher suite (TLS_DHE), Sequence number (1), Client write encryption key, Client write MAC key (16BAD1), Server write encryption key, Server write MAC key (4D017), and Pending state.
- Messages Panel:** Displays the message flow. The "[Handshake] finished" message is highlighted in green, and the "[ChangeCipher Spec]" message is highlighted in yellow. The "Stream fragment" is also visible. Below these, the "Bytes" tab shows the details of the TLS handshake, including the Content Type (Handshake), Version (3,3) TLS 1.2, Length (40), and the AEAD fragment (Nonce explicit 0x0000000000000000, Content TLSHandshake, HandshakeType finished, Length 12, Body finished, VerifyData 0x84D50B23D7EA9464CF).
- Server Panel:** Shows the state of the server during the handshake. The "Current read state" and "Current write state" are highlighted in yellow. The state list includes: Session ID (0xE26786EC21), Client random (0x561CD09), Server random (0x561CD0), Pre master secret (0x18F), Master secret (0x3642FB5), Certificate, DH parameters (dh_p 0x00FCA682CE8E1, dh_g 0x678471B27A9CF, dh_Ys 0x77D3682C88B9, dh_Yc 0x5F4BA46F3538), Current read state, Current write state, and Pending state.

At the bottom of the application, there are buttons for "Show info", "Next message", and "All messages".

Possible next Steps



Thank you!