Integrate Fish and Begol in TLS

Advisor(s): Sebastian Ramacher

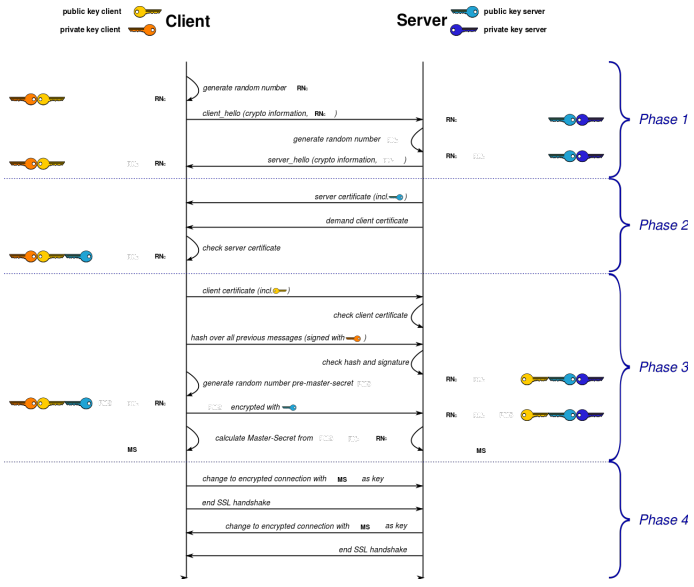
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

During the initial handshake, TLS relies heavily on signature schemes to authenticate the identity of the peers. All signature schemes that are currently in use in TLS are easily broken by sufficiently powerful quantum computers. In view of the steady progress in constructing real-world quantum computers, these schemes need to be replaced with post-quantum secure ones. Two candidates for post-quantum secure schemes are Fish and Begol which solely rely on symmetric-key primitives such as block ciphers and hash functions.

Goals and Tasks

- Get familiar with the signature schemes.
- Understand the TLS handshake.
- Integrate the signature schemes in a TLS library.



TLS handshake (CC-BY 3.0)

Literature

- D. Derler et al.
  Digital Signatures from Symmetric-Key Primitives
  preprint
- T. Dierks and E. Rescorla
  The Transport Layer Security (TLS) Protocol Version 1.2
  RFC 5246 (Proposed Standard) 2008
  http://www.ietf.org/rfc/rfc5246.txt

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Basic cryptographic background
- C/C++ programming

Advisor / Contact

sebastian.ramacher@iaik.tugraz.at.