Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Module: CO-566
Date: 2022-04-07
Due: 2022-04-21

SADS 2022 Problem Sheet #9

Problem 9.1: *secure TLS connection establishment* (8+2 = 10 points)

Implement a TLS client in C or Rust that establishes a secure TLS connection with a server (for example, `www.example.com`), checks the server's certificate, enforces the minimal version of TLS 1.2 and gracefully closes the connection. The certificate check must include

- a check of the certificate expiration date,
- a check whether the certificate name matches the expectation,
- a check of the validity of the signature chain, and
- a check of the revocation status (either by CRL or OCSP).

Use the default OS certificate store as the trust anchor. You can choose from any of the following TLS libraries:

- OpenSSL
- LibreSSL
- GnuTLS
- wolfSSL
- Mbed TLS
- Rustls
- Rust native-tls

You may use `https://badssl.com` and `https://revoked.grc.com/` for testing purposes.

a) Implementat a program establishing (and closing) a secure TLS connection as described above.

b) Write a reflection of the usability of the API that you have used and its documentation. Explain which aspects of the task turned out to be more complicated than expected and how the API could potentially be improved.