Advanced Networking
Università della Svizzera italiana — A. Carzaniga, P. Polverino

Assignment n. 5 (graded)
May 24, 2024

Assignment 5: Simple TLS

Due date: *Sunday, June 2, 2024 at 22:00*

> *This is an individual assignment. You may discuss it with others, but your code and documentation must be written on your own.*

Create a simple implementation of a TLS 1.2 client in the C language. You are provided with a project setup that you can use to create such an implementation. The project setup is available on the iCorsi system. To complete the client implementation, you should complete all the TODO tasks you will find within the code. All the TODO tasks will be in the `tls_impl.c` source file. The project also contains a test suite that you can run using the `make check` command to check the correctness of your implementation. The project Makefile also includes a rule to run the test with Valgrind to help you detect possible memory leaks in your implementation. To run the tests with Valgrind, use the `make check-valgrind` command. To build the entire project, run the `make` command. Note that the tool also builds a TLS server that you can use to validate your implementation. The client program is already implemented for you. The client will try to connect to the server, and it will ping it. Upon receiving a connection from a client, the server will reply with a pong message, and it will close the connection. Note that you do not have to implement the entire protocol, and instead you just need to support one cipher suite, namely TLS_RSA_WITH_AES_128_CBC_SHA256. On the iCorsi system you should also be able to find some notes about the TLS 1.2 protocol and how to use the OpenSSL cryptography library.

Submission Instructions

Submit only the `tls_impl.c` through the iCorsi system. Add comments to your code to explain sections of the code that might not be clear. You must also add comments at the beginning of the source file to properly acknowledge any and all external sources of information you may have used, including code, suggestions, and comments from other students. If your implementation has limitations and errors you are aware of (and were unable to fix), then list those as well in the initial comments.

You may use an integrated development environment (IDE) of your choice. However, *do not submit any IDE-specific file*, such as project description files.