Socket Programming Phase 3

公衛三 陳佳雯 b07801004

Environment

Ubuntu 20.04.1 LTS (on Windows 10 WSL)

Language

c++, c

Compile & Execute

In terminal (Ubuntu \ windows Powershell wsl), type in `cd /[file's name]` to change direction to file directory.

1. Type in `make -f makefile.cli` command, and then `client` binary file will appear.
2. Or type in `make -f makefile.ser` command, and then `server` binary file will appear.
3. After successful compilation, type in `./client` or `./server` command to execute binary file in terminal separately.
4. Follow the instructions on the screen.

Phase 3 New Features

1. Microtransaction with peers
2. Server updates client's balances according to the transaction amount.
3. SSL encryption between client and client
4. SSL encryption between client and server
5. Auto create certificate and key

Description

Microtransaction with peers

- Scenario:

  payer A wants to transact with payee B

- Design:

  A sends the transaction message to B →

  A sends the transaction message to server →

  Server update A's balance and B's balance

SSL encryption

- For every socket which needs ssl encryption, it will use functions bellow:

  InitClientCTX()

  → Use SSLv23_client_method() to initialize SSL Content Text

  InitServerCTX() → Use SSLv23_server_method() to initialize SSL Content Text

  LoadCertificates(SSL_CTX* ctx)

  → load user's certificate & load user's private key & check correctness of private key

```
SSL_CTX* InitClientCTX();
SSL_CTX* InitServerCTX();
void LoadCertificates(SSL_CTX* ctx);
void ShowCerts(SSL *ssl);
```

Auto create certificate and key

Exception Handling

Reference

SSL_CTX:
https://www.openssl.org/docs/man1.0.2/man3/SSL_CTX_use_certificate_file.html

- Create certificate and key dynamically:
  https://stackoverflow.com/questions/256405/programmatically-create-x509-certificate-using-openssl