

Socket programming HW3

資管五 徐遠志 b05705046

- 如何 Compile

開啟 terminal 然後 cd 到有 server_main.cpp 的目錄下，執行：

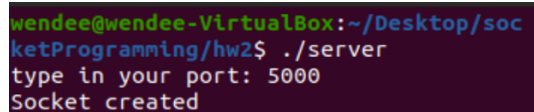
```
make
```

- 如何執行程式 (包含參數說明)

在 terminal 執行：

```
./server
```

接著程式會問 server 要聽哪一個 port，就輸入 port:



```
wendee@wendee-VirtualBox:~/Desktop/socketProgramming/hw2$ ./server
type in your port: 5000
Socket created
```

看到 Socket created 就表示成功了

開另一個 terminal 視窗，執行：

```
./client
```

程式會先問 host 要聽哪一個 port (for communicating with server)，下一個問 client communication 要聽哪一個 port (for transfer money between clients)，分別輸入就可以了。

- 程式需求、執行需求或環境

虛擬機器安裝 linux 20.04 版本的 ISO 檔

需要 g++ 進行編譯

- 程式邏輯說明與截圖搭配

由於這次需要做安全傳輸，所以資料夾裡應該會有 x.crt 和 x.key，分別是自簽憑證和私鑰，在建立 socket 之前，我們會先初始化安全傳輸設定：

```
SSL_CTX* initCTXServer(void)
{
    SSL_CTX *ctx;
    const SSL_METHOD *ssl_method;

    SSL_library_init();
    SSL_load_error_strings();
    ssl_method = SSLv23_method();
    ctx = SSL_CTX_new(ssl_method);
    if(ctx == NULL)
    {
        ERR_print_errors_fp(stderr);
        abort();
    }
    return ctx;
}
```

接著會利用 SSL 內建函式來驗證憑證：

```
SSL_CTX* initCTXServer(void)
{
    SSL_CTX *ctx;
    const SSL_METHOD *ssl_method;

    SSL_library_init();
    SSL_load_error_strings();
    ssl_method = SSLv23_method();
    ctx = SSL_CTX_new(ssl_method);
    if(ctx == NULL)
    {
        ERR_print_errors_fp(stderr);
        abort();
    }
    return ctx;
}
```

有了初始化和憑證驗證，我們接著只要把 socket 建立在 ssl 上就可以了

```
ctx1 = client.initCTX();
client.Certify(ctx1, CLIENT_B_CERT, CLIENT_B_PRI);
ssl1 = SSL_new(ctx1);
SSL_set_fd(ssl1, socket_transfer);

if(SSL_connect(ssl1) <= 0)
|   ERR_print_errors_fp(stderr);
else
{
|   client.receive(ssl1);
|   client.send_data(ssl1, command);
}

SSL_free(ssl1);
close(socket_transfer);
```

因為這次主要需要實作轉帳功能，為了預防轉帳對象不在線上、交易金額大於轉出帳戶的問題，我們會先把訊息傳給 server，透過 server 檢查一切無誤後，他會回傳 1 0 0 O K，此時對方就會正確收到欲轉出之金額

```
string command;
bool isTransactionOK = false;
while (!isTransactionOK)
{
|   cout << "command: ";
|   cin >> command;
|   client.send_data(client.GetHostSSL(), "TRANS#" + command);
|   string response = client.receive(client.GetHostSSL());
|   isTransactionOK = contains(response, "100");
}
```