网络安全课程实验

题目：SSL 保护的 C-S 发信程序设计

学　　院 计算机与电子信息学院

专　　业 信息安全

班　　级 [redacted]

姓　　名 [redacted]

学　　号 [redacted]

2020　年　6　月 26 日

一、 实验目的

开发一个客户端程序和一个服务器程序。客户端可以将文件中的数据发送到服务器。必须使用 ssl 保护网络中传输的数据。

二、 程序设计思路

为实现使用 SSL 进行 SOCKET 套接字的保护，使用 openssl 提供的 API 进行了程序编写，实现了实验目的。

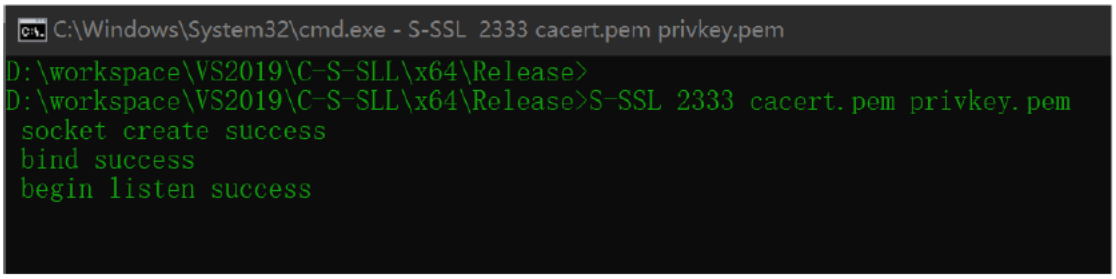
为了进行在 SSL 保护下的 SOCKET 套接字通讯，需要进行以下步骤：

1、初始化 SSL 环境
2、选择会话协议
3、创建会话环境
4、建立 SSL 套接字
5、完成 SSL 握手
6、进行数据传输
7、结束 SSL 通讯

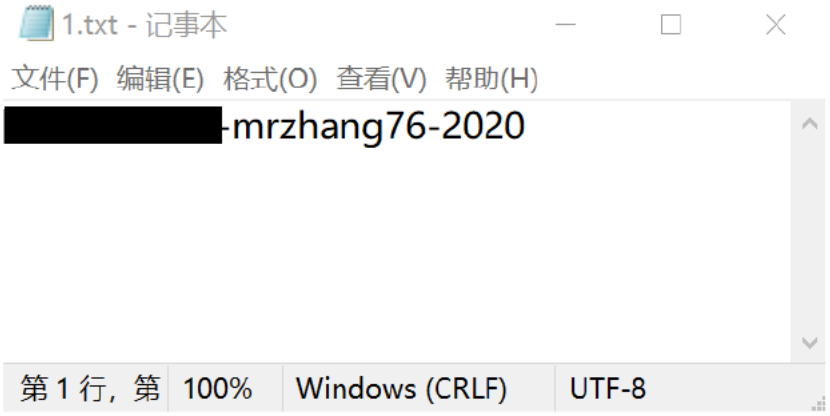
实验中使用了 openssl 生成的密钥证书进行测试。

三、 程序测试

1、启动服务器端开始监听



2、启动客户端传输文件数据



```
D:\workspace\VS2019\C-S-SLL\x64\Release>C-SSL 127.0.0.1 2333 1.txt
socket creat success
address creat success
server connect success
Connected with TLS_AES_256_GCM_SHA384 encryption
Digital certificate information:
certificate: /C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
lusser: /C=AU/ST=Some-State/O=Internet Widgits Pty Ltd
Message received successfully:  SERVER LISTENING...  The length of data: 21
Message received successfully: 1707310316-mrzhang76-2020 The length of data: 25

D:\workspace\VS2019\C-S-SLL\x64\Release>
```

3、服务器接收到数据

```
C:\Windows\System32\cmd.exe - S-SSL  2333 cacert.pem privkey.pem
D:\workspace\VS2019\C-S-SLL\x64\Release>
D:\workspace\VS2019\C-S-SLL\x64\Release>S-SSL 2333 cacert.pem privkey.pem
 socket create success
 bind success
 begin listen success
 SERVER GET CONNECTION FROM: 127.0.0.1 PORT: 51875 SOCKET: 276
 SEND INFORMATION:  SERVER LISTENING...  SUCCESS, INFORMATION LEN: 21
 RECEIVE INFORMATION SUCCESS: 1707310316-mrzhang76 INFORMATION LEN: 1
 SERVER GET CONNECTION FROM: 127.0.0.1 PORT: 54237 SOCKET: 276
 SEND INFORMATION:  SERVER LISTENING...  SUCCESS, INFORMATION LEN: 21
 RECEIVE INFORMATION SUCCESS: 1707310316-mrzhang76 INFORMATION LEN: 1
 SERVER GET CONNECTION FROM: 127.0.0.1 PORT: 54266 SOCKET: 280
 SEND INFORMATION:  SERVER LISTENING...  SUCCESS, INFORMATION LEN: 21
 RECEIVE INFORMATION SUCCESS:  [redacted]-mrzhang76-2020 INFORMATION LEN: 1
```

四、 实验结论

本实验通过编写 c++代码，实现了使用 SSL 保护 socket 套接字的通讯。