**北京科技大学实验报告**

学院：计通学院 专业：信息安全 班级：信安182

姓名：王泽辰 学号：41824180 实验日期：2020年12月16日

**实验名称：**

调研并尝试  ssl 双向认证的代码实现

**实验内容与步骤：**

我们常见的SSL验证较多的只是验证我们的服务器是否是真实正确的，当然如果你访问的URL压根就错了，那谁也没有办法。这个就是所谓的SSL单向认证。

但是实际中，我们有可能还会验证客户端是否符合要求，也就是给我们每个用户颁发一个证书，比且每个数字证书都是唯一的，不公开的。这样就能通过这个数字证书保证当前访问我服务器的这个用户是经过服务器认可的，其他人不可访问。

双向认证 从第一个层面上 确保了服务器 与客户端 都是互相认可的。那么他们之间要进行通信，就会在通信协议上附加SSL协议，确保通信的内容是加密的，即使是sniffer这样的网络嗅探工具看到的都是乱码。以后给大家演示下不加密的情况下，用sniffer看到的是什么。恐怕这样你就能提高警惕了。

以下内容从网络上摘抄 加以实际验证后修改的。

模拟场景：

Server端和Client端通信，需要进行授权和身份的验证，即Client只能接受Server的消息，Server只能接受Client的消息。

实现技术：

JSSE（Java Security Socket Extension）

是Sun为了解决在Internet上的安全通讯而推出的解决方案。它实现了SSL和TSL（传输层安全）协议。在JSSE中包含了数据加密，服务器验证，消息完整性和客户端验证等技术。通过使用JSSE，开发人员可以在客户机和服务器之间通过TCP/IP协议安全地传输数据。

为了实现消息认证。

Server需要：

1）KeyStore: 其中保存服务端的私钥

2）Trust KeyStore:其中保存客户端的授权证书

同样，Client需要：

1）KeyStore：其中保存客户端的私钥

2）Trust KeyStore：其中保存服务端的授权证书

在这里我还是推荐使用Java自带的keytool命令，去生成这样信息文件。当然目前非常流行的开源的生成SSL证书的还有OpenSSL。OpenSSL用C语言编写，跨系统。但是我们可能在以后的过程中用java程序生成证书的方便性考虑，还是用JDK自带的keytool。

1）生成服务端私钥，并且导入到服务端KeyStore文件中

keytool -genkey -alias serverkey -keystore kserver.keystore

过程中，分别需要填写

keystore密码：w1z2c3

名字和姓氏：wzc

组织单位名称：wzc

组织名称：wzc

城市或区域名称：wzc

州或省份名称：wzc

国家代码：wzc

serverkey私钥的密码，不填写和keystore的密码一致。这里千万注意，直接回车就行了，不用修改密码。否则在后面的程序中以及无法直接应用这个私钥，会报错。

就可以生成kserver.keystore文件

server.keystore是给服务端用的，其中保存着自己的私钥

2）根据私钥，导出服务端证书

keytool -export -alias serverkey -keystore kserver.keystore -file server.crt

server.crt就是服务端的证书

3）将服务端证书，导入到客户端的Trust KeyStore中

keytool -import -alias serverkey -file server.crt -keystore tclient.keystore

tclient.keystore是给客户端用的，其中保存着受信任的证书

采用同样的方法，生成客户端的私钥，客户端的证书，并且导入到服务端的Trust KeyStore中

1）keytool -genkey -alias clientkey -keystore kclient.keystore

2）keytool -export -alias clientkey -keystore kclient.keystore -file client.crt

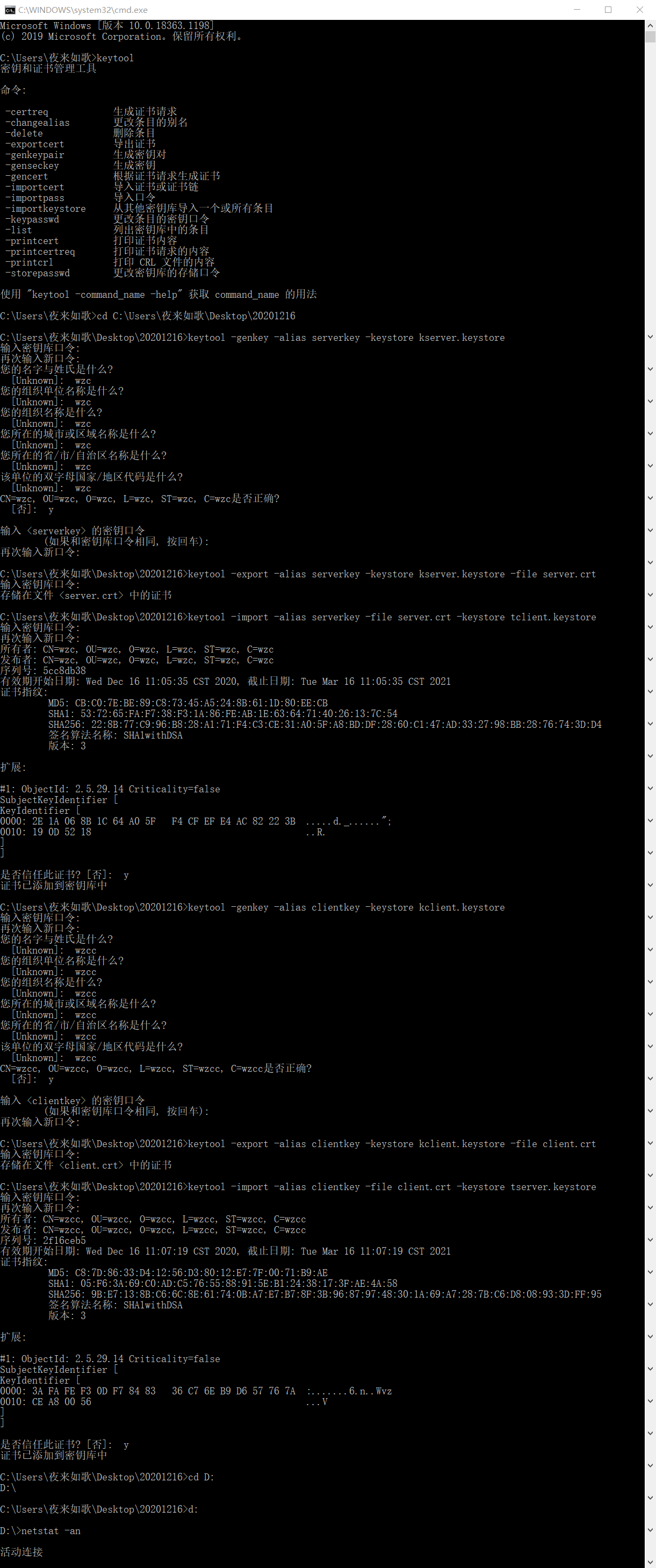
3）keytool -import -alias clientkey -file client.crt -keystore tserver.keystore

如此一来，生成的文件分成两组

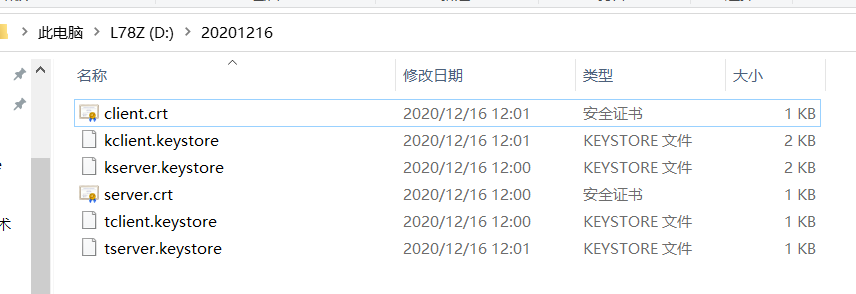
服务端保存：kserver.keystore tserver.keystore

客户端保存：kclient.keystore  tclient.kyestore

生成过程如下：



文件夹内容：



JAVA验证源码在文件夹内。