

# openssl 编程入门（含完整示例）

易剑

## 1. 编写目的

第一次跑起 openssl 示例并不太简单，本文的目的是为了让这个过程变得非常简单。在开始之前，要非常感谢[周立发](#)同学，正是通过他共享的示例，较轻松的入了门。本文档对他共享的示例中的一个小错误进行了修正，并提供了傻瓜式的“编译-生成-KEY 运行”一条龙脚本（[方法请参见压缩包中的 readme 文件](#)），让跑第一个 openssl 程序变得轻轻松松。

## 2. 示例包



ssl\_test.tar.gz



openssl-0.9.8h-SuSE10.tar.gz

ssl\_test.tar.gz 为示例源代码包，openssl-0.9.8h-SuSE10.tar.gz 为 openssl 二进制包，测试时是安装在/usr/local/ssl。

ssl\_test.tar.gz 中的示例在 SuSE10中测试通过，使用的是 openssl-0.9.8h，它包括如下文件：

```
-rw-r--r-- 1 root root 1346 Dec 5 18:11 cacert.pem
-rwxr-xr-x 1 root root 114 Dec 5 18:11 make_key.sh
-rwxr-xr-x 1 root root 172 Dec 5 18:37 mk_client.sh
-rwxr-xr-x 1 root root 172 Dec 5 18:37 mk_server.sh
-rw-r--r-- 1 root root 1679 Dec 5 18:11 privkey.pem
-rw-r--r-- 1 root root 167 Dec 5 18:39 readme
-rwxr-xr-x 1 root root 38 Dec 5 18:38 run_client.sh
-rwxr-xr-x 1 root root 64 Dec 5 18:38 run_server.sh
-rwxr-xr-x 1 root root 1140142 Dec 5 18:38 ssl_client
-rw-r--r-- 1 root root 3928 Dec 5 17:31 ssl_client.cpp
-rwxr-xr-x 1 root root 1139667 Dec 5 18:38 ssl_server
-rw-r--r-- 1 root root 4882 Dec 5 17:31 ssl_server.cpp
```

readme 为包内容说明，run\_server.sh 用来运行服务端，run\_client.sh 用来运行客户端，mk\_server.sh 用来编译服务端，mk\_client.sh 用来编译客户端，make\_key.sh 用来生成钥匙 KEY。

### 3. 什么是 SSL?

在学习 openssl 编程之前，先了解一下什么是 SSL，有助于后续的学习。SSL 是一个缩写，代表的是 **Secure Sockets Layer**。它是支持在 **Internet** 上进行安全通信的标准，并且将数据密码术集成到了协议之中。数据在离开您的计算机之前就已经被加密，然后只有到达它预定的目标后才被解密。证书和密码学算法支持了这一切的运转，使用 **OpenSSL**，您将有机会切身体会它们。

理论上，如果加密的数据在到达目标之前被截取或窃听，那些数据是不可能被破解的。不过，由于计算机的变化一年比一年快，而且密码翻译方法有了新的发展，因此，SSL 中使用的加密协议被破解的可能性也在增大。可以将 SSL 和安全连接用于 **Internet** 上任何类型的协议，不管是 **HTTP**、**POP3**，还是 **FTP**。还可以用 SSL 来保护 **Telnet** 会话。虽然可以用 SSL 保护任何连接，但是不必对每一类连接都使用 SSL。如果连接传输敏感信息，则应使用 SSL。

### 4. 什么是 openssl?

openssl 不仅仅是 SSL。它可以实现消息摘要、文件的加密和解密、数字证书、数字签名和随机数字。关于 OpenSSL 库的内容非常多，远不是一篇文章可以容纳的。OpenSSL 不只是 API，它还是一个命令行工具。命令行工具可以完成与 API 同样的工作，而且更进一步，可以测试 SSL 服务器和客户机。

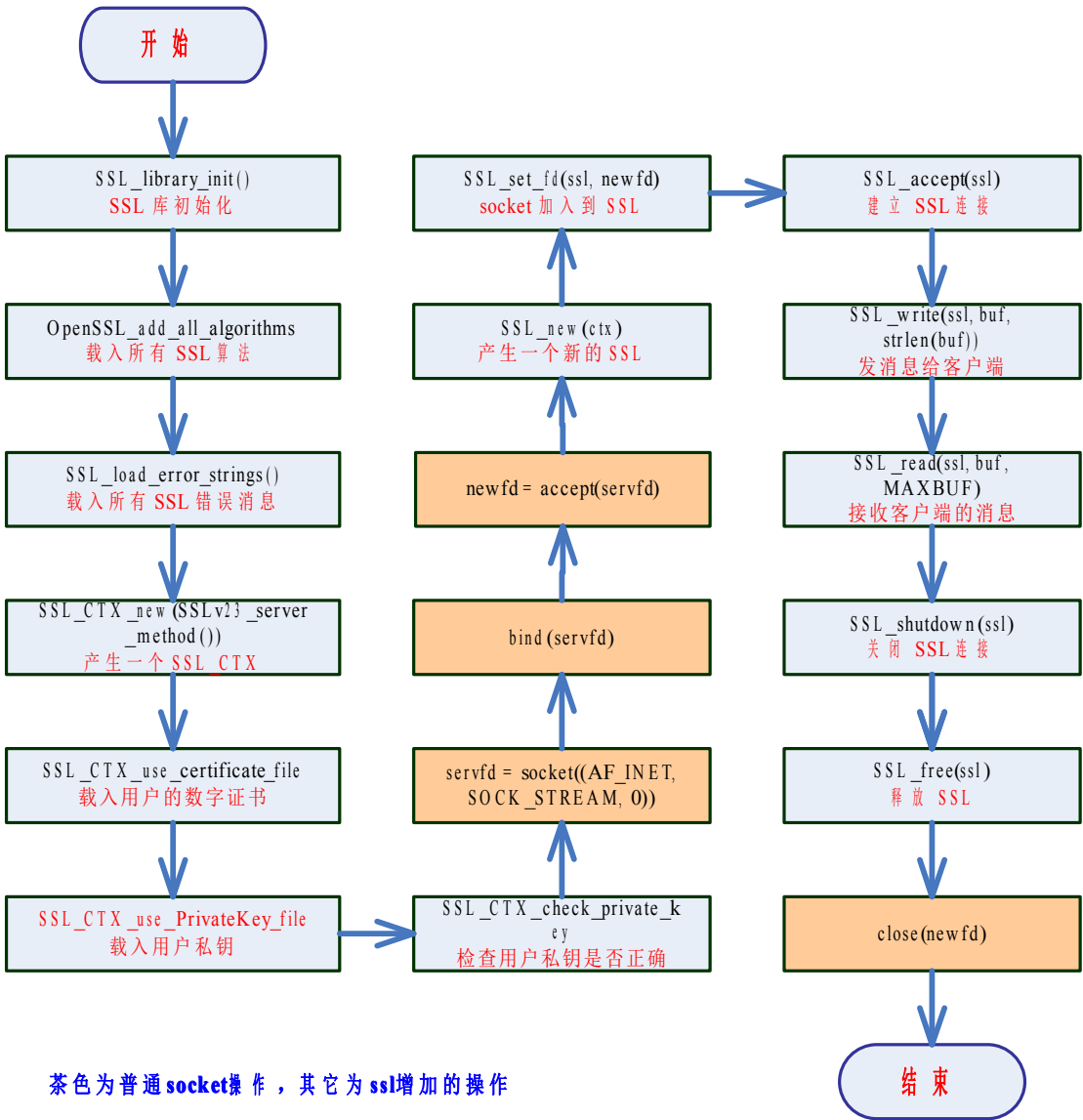
### 5. 示例程序

示例的说明请参见下面这篇[周立发](#)共享的文章。

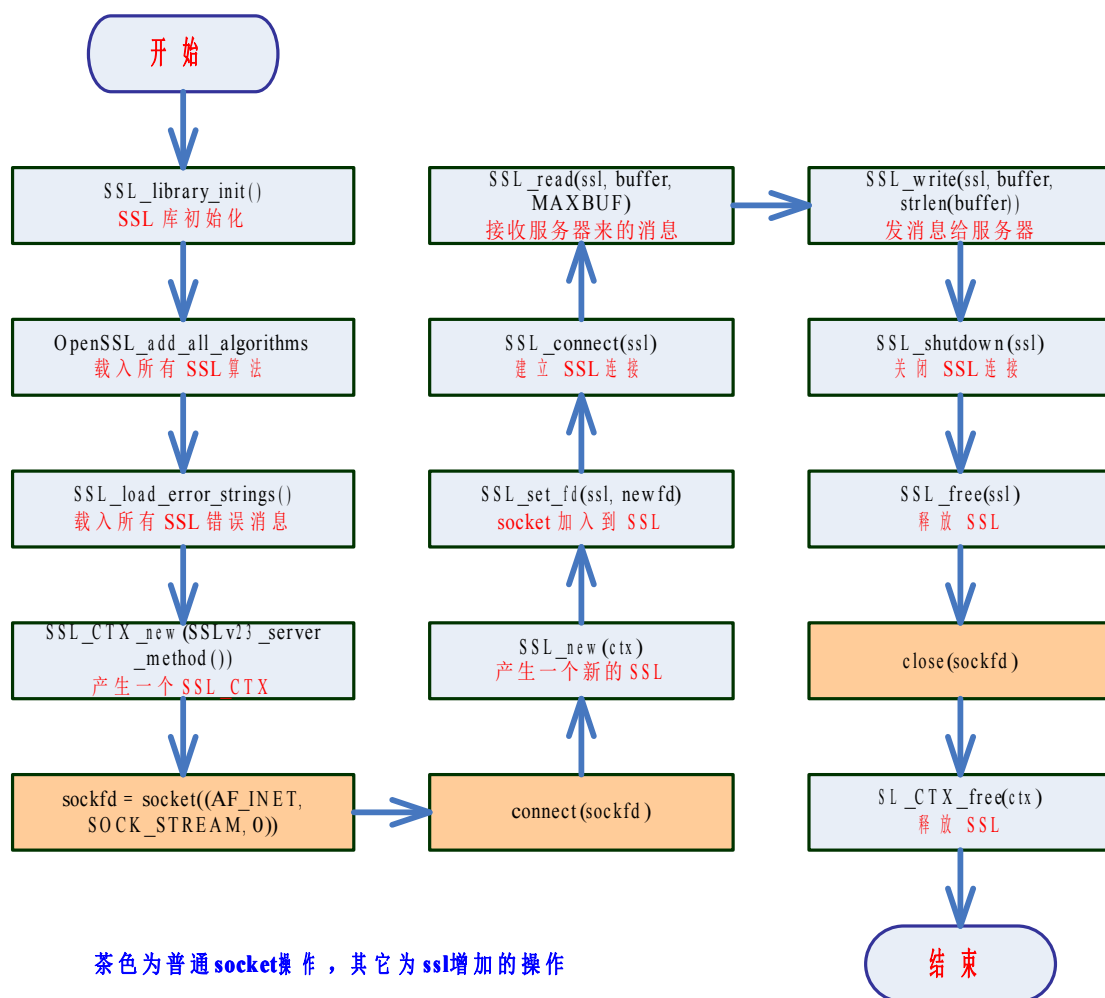


加密通讯协议SSL  
编程.pdf

6. 服务端编写步骤



## 7. 客户端编写步骤



## 8. 相关头文件

### 8.1. socket 头文件

```

#include <sys/types.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <sys/socket.h>

```

## 8.2. SSL 头文件

```
#include <openssl/ssl.h>
#include <openssl/err.h>
```

## 9. 结尾

上面步骤应当画得比较清楚了，结合图再对照 `ssl_test.tar.gz` 和《加密通讯协议 SSL 编程.pdf》就可以非常快地上手了。