



一篇文章让你彻底弄懂SSL/TLS协议

 **flydean**
程序那些事

关注他

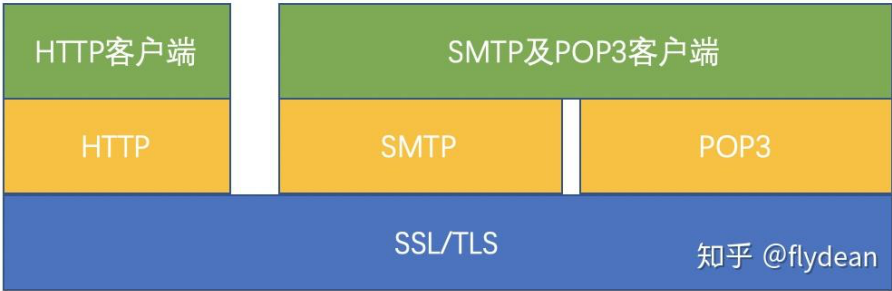
304 人赞同了该文章

SSL/TLS是一种密码通信框架，他是世界上使用最广泛的密码通信方法。SSL/TLS综合运用了密码学中的对称密码，消息认证码，公钥密码，数字签名，伪随机数生成器等，可以说是密码学中的集大成者。

SSL(Secure Socket Layer)安全套接层，是1994年由Netscape公司设计的一套协议，并与1995年发布了3.0版本。

TLS(Transport Layer Security)传输层安全是IETF在SSL3.0基础上设计的协议，实际上相当于SSL的后续版本。

SSL/TLS的应用



SSL/TLS是一个安全通信框架，上面可以承载HTTP协议或者SMTP/POP3协议等。

TLS协议的架构



TLS主要分为两层，底层的是TLS记录协议，主要负责使用对称密码对消息进行加密。

上层的是TLS握手协议，主要分为握手协议，密码规格变更协议和应用数据协议4个部分。

- 握手协议负责在客户端和服务端商定密码算法和共享密钥，包括证书认证，是4个协议中最复杂的部分。
- 密码规格变更协议负责向通信对象传达变更密码方式的信号
- 警告协议负责在发生错误的时候将错误传达给对方
- 应用数据协议负责将TLS承载的应用数据传达给通信对象的协议。

握手协议

握手协议是TLS协议中非常重要的协议，通过客户端和服务端的交互，和共享一些必要信息，从而生成共享密钥和交互证书。

不说话，先上图：

接下来我们一步步的介绍每一步的含义：

1. client hello客户端向服务器端发送一个client hello的消息，包含下面内容：

- 可用版本号
- 当前时间
- 客户端随机数
- 会话ID
- 可用的密码套件清单
- 可用的压缩方式清单

我们之前提到了TLS其实是一套加密框架，其中的有些组件其实是可以替换的，这里可用版本号，可用的密码套件清单，可用的压缩方式清单就是向服务器询问对方支持哪些服务。

客户端随机数是一个由客户端生成的随机数，用来生成对称密钥。

1. server hello服务器端收到client hello消息后，会向客户端返回一个server hello消息，包含如下内容：

- 使用的版本号
- 当前时间
- 服务器随机数
- 会话ID
- 使用的密码套件
- 使用的压缩方式

使用的版本号，使用的密码套件，使用的压缩方式是对步骤1的回答。

服务器随机数是一个由服务器端生成的随机数，用来生成对称密钥。

1. 可选步骤:certificate服务器端发送自己的证书清单，因为证书可能是层级结构的，所以处理服务器自己的证书之外，还需要发送为服务器签名的证书。

客户端将会对服务器端的证书进行验证。如果是匿名的方式通信则不需要证书。

2. 可选步骤:ServerKeyExchange

如果第三步的证书信息不足，则可以发送ServerKeyExchange用来构建加密通道。

ServerKeyExchange的内容可能包含两种形式：

- 如果选择的是RSA协议，那么传递的就是RSA构建公钥密码的参数（E，N）。我们回想一下RSA中构建公钥的公式： $\text{密文} = \text{明文}^E \bmod N$ ，只要知道了E和N，那么就知道了RSA的公钥，这里传递的就是E，N两个数字。具体内容可以参考[RSA算法详解](#)
- 如果选择的是Diff-Hellman密钥交换协议，那么传递的就是密钥交换的参数，具体内容可以参考[更加安全的密钥生成方法Diffie-Hellman](#)

1. 可选步骤:CertificateRequest如果是在一个受限访问的环境，比如fabric中，服务器端也需要向客户端索要证书。

如果并不需要客户端认证，则不需要此步骤。

2. server hello done

服务器端发送server hello done的消息告诉客户端自己的消息结束了。

3. 可选步骤:Certificate

对步骤5的回应，客户端发送客户端证书给服务器

4. ClientKeyExchange

还是分两种情况：

- 如果是公钥或者RSA模式情况下，客户端将根据客户端生成的随机数和服务器端生成的随机数，生成预备主密码，通过该公钥进行加密，返送给服务器端。
- 如果使用的是Diff-Hellman密钥交换协议，则客户端会发送自己这一方要生成Diff-Hellman密钥而需要公开的值。具体内容可以参考[更加安全的密钥生成方法Diffie-Hellman](#)，这样服务器端可以根据这个公开值计算出预备主密码。

1. 可选步骤:CertificateVerify客户端向服务器端证明自己是客户端证书的持有者。

2. ChangeCipherSpec(准备切换密码)

ChangeCipherSpec是密码规格变更协议的消息，表示后面的消息将会以前面协商过的密钥进行加密。

3. finished(握手协议结束)

客户端告诉服务器端握手协议结束了。

4. ChangeCipherSpec(准备切换密码)

服务器端告诉客户端自己要切换密码了。

5. finished(握手协议结束)

服务器端告诉客户端，握手协议结束了。

6. 切换到应用数据协议

这之后服务器和客户端就是以加密的方式进行沟通了。

主密码和预备主密码

上面的步骤8生成了预备主密码，主密码是根据密码套件中定义的单向散列函数实现的伪随机数生成器+预备主密码+客户端随机数+服务器端随机数生成的。

主密码主要用来生成称密码的密钥，消息认证码的密钥和对称密码的CBC模式所使用的初始化向量。详见[分组密码和模式](#)

TLS记录协议

TLS记录协议主要负责消息的压缩，加密及数据的认证：

先上图。

消息首先将会被分段，然后压缩，再计算其消息验证码，然后使用对称密码进行加密，加密使用的是CBC模式，CBC模式的初始向量是通过主密码来生成的。

得到密文之后会附加类型，版本和长度等其他信息，最终组成最后的报文数据。

更多内容请访问 [flydean的博客](#)

发布于 2020-04-19 00:41

[SSL](#) [HTTPS](#) [SSL 证书](#)



欢迎参与讨论

30 条评论

默认 最新



至尊宝

不是很明白，明明是应用层的协议非得叫Transport Layer Security🤔

2022-10-20

回复 1

- 

西门宅宅

作者的意思是不是在tcp上面，但是又不到http层？

2023-03-23

回复 1
- 

唐虎 flydean

在7层架构里，SSL和TLS属于会话层；在5层架构里，是合并到应用层里的，在应用层里是贴着传输层的，名字里带个transport也可以理解。

04-10

回复 喜欢
- 展开其他 1 条回复 >
- 

顾挺

ssl加密 内容被加密了 ip还是可以被识别吗？

2021-11-11

回复 1
- 

游客

ssl 加密是在表现层，此时还没有 ip 头，ip头是在 ip 层才有的，所以不影响。

2022-01-02

回复 11
- 

木小觞 

作者知道AKMA么，想知道AKMA和TLS协议是不是两个不同的概念，之间的关系大概像独立的同等级的两个东西（虽然会有小的交集）

2021-04-27

回复 喜欢
- 

flydean 作者

不知道呀

01-19

回复 喜欢
- 

我比多肉更多肉

校园网无法自转登录界面

2022-06-10

回复 喜欢
- 

flydean 作者

这个问题解答不了你

01-19

回复 喜欢
- 

周旭

写的很好! 解惑了!

2020-06-08

回复 1
- 

flydean 作者

不客气

2020-06-08

回复 1
- 

n123

大佬，“上层的是TLS握手协议，主要分为握手协议，密码规格变更协议和应用数据协议4个部分”这句话是不是有点问题

2021-02-02

回复 1
- 

flydean 作者

可以把 TLS握手协议看做是一个统称



2021-02-02

回复 3
- 

风暴洋

也就是说客户端是必须要验证服务器的证书，但服务器可以不验证客户端的证书，是吗？

2023-06-18

回复 喜欢

**CodeY**

开启双向认证就会验证客户端的证书

2023-09-04

 回复  喜欢

**CodeY**

对

2023-09-04

 回复  喜欢

**VANHOPE**

感谢楼主！

2022-10-25

 回复  喜欢

**flydean** 作者

不客气

01-19

 回复  喜欢

**旋风**

心跳协议呢

2021-10-25

 回复  喜欢

**flydean** 作者

ping pong的那种吗？

01-19

 回复  喜欢

**雪野秋**

如果服务端向客户端发送了证书，那客户端需要返回的就是通过公钥加密的客户端随机数了呀，预备主密码是在服务端证书信息不全的情况下需要传递的内容吗？

2021-09-08

 回复  喜欢

**Kevin Durant**

预备主密码不是服务端证书信息不全的情况下传递的内容，是密钥交换必须要完成的握手步骤。证书的作用是身份认证而不是密钥协商。

2022-03-31

 回复  2


**flydean** 作者

可以看看Diffie-Hellman算法

01-19


 回复  喜欢


点击查看全部评论 >



欢迎参与讨论

文章被以下专栏收录

- 

程序那些事
懂程序，更懂你！
- 

Chemistry (Pharmacy)
LearningChemistryPharmacy

推荐阅读

浏览器地址栏显示效果

安全锁

https://www.yourdomain.com

yourdomain.com

eg.
(any.yourdomain.com)
(every.yourdomain.com)
(www.yourdomain.com)

• 企业信息验证

• 所有子域可用

• 节约部署成本

SSL证书的生产方法

格林

SSL：证书文件

大川搬砖

发表于SSL（T...

ECC vs RSA

椭圆曲线加密算法(ECC)非对称加密算法(RSA)

256位

效果等同

3072位

ECC作为SSL/TLS证书加密算
法的优势

上海哲信息技术有限公司

自签SSL证书以及https的
认证

沐枫

发表于沐枫1

▲ 赞同 304 ▼ 30 条评论 ↗ 分享 ❤ 喜欢 ★ 收藏 📄 申请转载 ...

