<https://blog.csdn.net/enweitech/article/details/81781405>

# HTTPS、SSL、TLS三者之间的联系和区别

2018年08月17日 17:52:54 [天府云创](https://me.csdn.net/English0523) 阅读数：1123

版权声明：本文为EnweiTech原创文章，未经博主允许不得转载。 https://blog.csdn.net/English0523/article/details/81781405

SSL(Secure Socket Layer 安全套接层)是基于HTTPS下的一个协议加密层，最初是由网景公司（Netscape）研发，后被IETF（The Internet Engineering Task Force - 互联网工程任务组）标准化后写入（RFCRequest For Comments 请求注释），RFC里包含了很多互联网技术的规范！

起初是因为HTTP在传输数据时使用的是明文（虽然说POST提交的数据时放在报体里看不到的，但是还是可以通过抓包工具窃取到）是不安全的，为了解决这一隐患网景公司推出了SSL安全套接字协议层，SSL是基于HTTP之下TCP之上的一个协议层，是基于HTTP标准并对TCP传输数据时进行加密，所以HPPTS是HTTP+SSL/TCP的简称。

由于HTTPS的推出受到了很多人的欢迎，在SSL更新到3.0时，IETF对SSL3.0进行了标准化，并添加了少数机制(但是几乎和SSL3.0无差异)，标准化后的IETF更名为TLS1.0(Transport Layer Security 安全传输层协议)，可以说TLS就是SSL的新版本3.1，并同时发布“RFC2246-TLS加密协议详解”，如果想更深层次的了解TLS的工作原理可以去RFC的官方网站：www.rfc-editor.org，搜索RFC2246即可找到RFC文档！ ——以上就是历史背景

SSL 是指安全套接字层，简而言之，它是一项标准技术，可确保互联网连接安全，保护两个系统之间发送的任何敏感数据，防止网络犯罪分子读取和修改任何传输信息，包括个人资料。两个系统可能是指服务器和客户端（例如，浏览器和购物网站），或两个服务器之间（例如，含个人身份信息或工资单信息的应用程序）。

要说清楚 HTTPS 协议的实现原理，至少需要如下几个背景知识。  
1. 大致了解几个基本术语（HTTPS、SSL、TLS）的含义  
2. 大致了解 HTTP 和 TCP 的关系（尤其是“短连接”VS“长连接”）  
3. 大致了解加密算法的概念（尤其是“对称加密与非对称加密”的区别）  
4. 大致了解 CA 证书的用途   5.TCP通信协议的几次握手

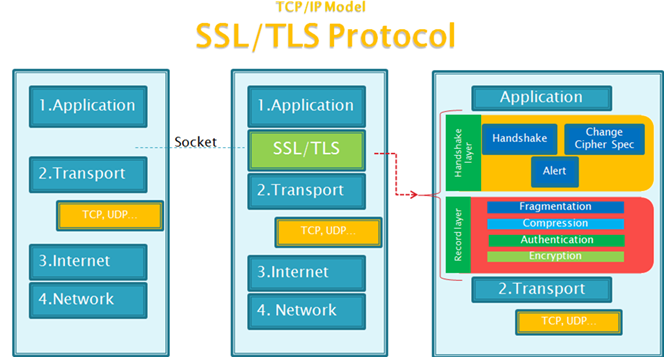
TLS（传输层安全）是更为安全的升级版 SSL。由于 SSL 这一术语更为常用，因此我们仍然将我们的安全证书称作 SSL。但当您从赛门铁克[购买 SSL](https://www.websecurity.symantec.com/zh/cn/ssl-certificate?inid=infoctr_buylink_sslhome) 时，您真正购买的是最新的 TLS 证书，有[ECC、RSA 或 DSA 三种加密方式](https://www.websecurity.symantec.com/zh/cn/security-topics/how-ssl-works)可以选择。

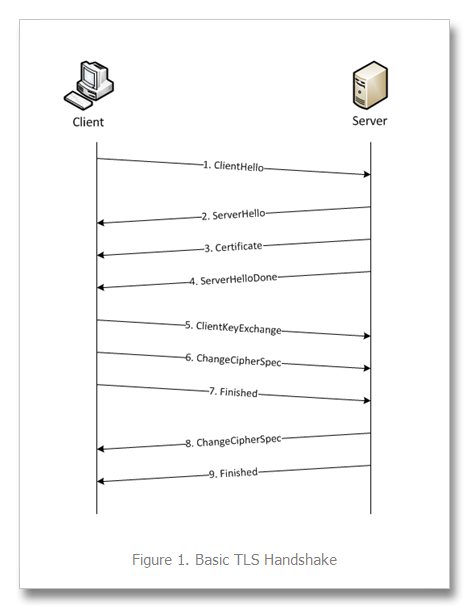
TLS/SSL是一种加密通道的规范  
  
它利用对称加密、公私钥不对称加密及其密钥交换算法，CA系统进行加密且可信任的信息传输  
  
在HTTP SSL中常用的对称加密算法有RC4,AES,3DES,Camellia等  
  
SSL由从前的网景公司开发  
有1,2,3三个版本，但现在只使用版本3  
  
TLS是SSL的标准化后的产物  
有1.0 1.1 1.2三个版本  
默认使用1.0  
  
TLS1.0和SSL3.0几乎没有区别  
  
事实上我们现在用的都是TLS，但因为历史上习惯了SSL这个称呼  
平常还是以SSL为多。

1. SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种[安全协议](https://www.baidu.com/s?wd=%E5%AE%89%E5%85%A8%E5%8D%8F%E8%AE%AE&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)。TLS与SSL在传输层对网络连接进行加密。
2. [SSL协议](https://www.baidu.com/s?wd=SSL%E5%8D%8F%E8%AE%AE&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)位于[TCP/IP协议](https://www.baidu.com/s?wd=TCP%2FIP%E5%8D%8F%E8%AE%AE&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)与各种应用层协议之间，为数据通讯提供安全支持。[SSL协议](https://www.baidu.com/s?wd=SSL%E5%8D%8F%E8%AE%AE&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)可分为两层： SSL记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。 SSL[握手协议](https://www.baidu.com/s?wd=%E6%8F%A1%E6%89%8B%E5%8D%8F%E8%AE%AE&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。
3. 安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成： TLS 记录协议（TLS Record）和 TLS [握手协议](https://www.baidu.com/s?wd=%E6%8F%A1%E6%89%8B%E5%8D%8F%E8%AE%AE&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)（TLS Handshake）。
4. TLS 的最大优势就在于：TLS 是独立于应用协议。高层协议可以透明地分布在 TLS 协议上面。然而，TLS 标准并没有规定应用程序如何在 TLS 上增加安全性；它把如何启动 TLS [握手协议](https://www.baidu.com/s?wd=%E6%8F%A1%E6%89%8B%E5%8D%8F%E8%AE%AE&tn=SE_PcZhidaonwhc_ngpagmjz&rsv_dl=gh_pc_zhidao)以及如何解释交换的认证证书的决定权留给协议的设计者和实施者来判断。

　1、SSL加密  
　　SSL是Netscape公司所提出的安全保密协议，在浏览器（如Internet Explorer、Netscape Navigator）和Web服务器（如Netscape的Netscape Enterprise Server、ColdFusion Server等等）之间构造安全通道来进行数据传输，SSL运行在TCP/IP层之上、应用层之下，为应用程序提供加密数据通道，它采用了RC4、MD5以及RSA等加密算法，使用40 位的密钥，适用于商业信息的加密。同时，Netscape公司相应开发了HTTPS协议并内置于其浏览器中，HTTPS实际上就是HTTP over SSL，它使用默认端口443，而不是像HTTP那样使用端口80来和TCP/IP进行通信。HTTPS协议使用SSL在发送方把原始数据进行加密，然后在接受方进行解密，加密和解密需要发送方和接受方通过交换共知的密钥来实现，因此，所传送的数据不容易被网络黑客截获和解密。 然而，加密和解密过程需要耗费系统大量的开销，严重降低机器的性能，相关测试数据表明使用HTTPS协议传输数据的工作效率只有使用HTTP协议传输的十分之一。假如为了安全保密，将一个网站所有的Web应用都启用SSL技术来加密，并使用HTTPS协议进行传输，那么该网站的性能和效率将会大大降低，而且没有这个必要，因为一般来说并不是所有数据都要求那么高的安全保密级别  
　　2、TLS加密  
　　TLS：安全传输层协议  
　　TLS：Transport Layer Security  
　　安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两层组成： TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。较低的层为 TLS 记录协议，位于某个可靠的传输协议（例如 TCP）上面。

### [SSL与TLS的区别以及介绍](https://www.cnblogs.com/susanhonly/p/7489532.html)





**SSL：（Secure Socket Layer，安全套接字层）**，位于可靠的面向连接的网络层协议和应用层协议之间的一种协议层。SSL通过互相认证、使用数字签名确保完整性、使用加密确保私密性，以实现客户端和服务器之间的安全通讯。该协议由两层组成：SSL记录协议和SSL握手协议。

**TLS：（Transport Layer Security，传输层安全协议）**，用于两个应用程序之间提供保密性和数据完整性。该协议由两层组成：TLS记录协议和TLS握手协议。

　　SSL是Netscape开发的专门用于保护Web通讯的，目前版本为3.0.最新版本的TLS 1.0是IETE（工程任务组）指定的一种新的协议，它建立在SSL 3.0协议规范之上，是SSL 3.0的后续版本。两者差别极小，可以理解为SSL 3.1，它是写入了RFC的。

**SSL（Secure Socket Layer）**

　　为Netscape所研发，用以保障在Internet上数据传输之安全，利用数据加密（Encryption）技术，可确保数据在网络上之传输过程中不会被截取。

　　当前版本为3.0。它已被广泛地用于Web浏览器与服务器之间的身份认证和加密数据传输。

　　SSL协议位于TCP/IP协议与各种应用层协议之间，为数据通讯提供安全支持。SSL协议可分为两层：SSL记录协议（SSL Record Protocol）：它建立在可靠的传输协议（如TCP）之上，为高层协议提供数据封装、压缩、加密等基本功能的支持。SSL握手协议（SSL Handshake Protocol）：它建立在SSL记录协议之上，用于在实际的数据传输开始前，通讯双方进行身份认证、协商加密算法、交换加密密钥等。

**SSL协议提供的服务主要有：**

　　1）认证用户和服务器，确保数据发送到正确的客户机和服务器；

　　2）加密数据以防止数据中途被窃取；

　　3）维护数据的完整性，确保数据在传输过程中不被改变。

**SSL协议的工作流程：**

　　服务器认证阶段：

　　1）客户端向服务器发送一个开始信息“Hello”以便开始一个新的会话连接；

　　2）服务器根据客户的信息确定是否需要生成新的主密钥，如需要则服务器在响应客户的“Hello”信息时将包含生成主密钥所需的信息；

　　3）客服根据收到的服务器响应信息，产生一个主密钥，并用服务器的公开密钥加密后传给服务器；

　　4）服务器恢复该主密钥，并返回给客户一个用主密钥认证的信息，以此让客户认证服务器。

　　用户认证阶段：在此之前，服务器已经通过了客户认证，这一阶段主要完成对客户的认证。经认证的服务器发送一个提问给客户，客户则返回（数字）签名后的提问和其公开密钥，从而向服务器提供认证。

　　TLS（Transport Layer Security Protocol）：安全传输层协议

　　安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。该协议由两成组成：TLS记录协议（TLS Record）和TLS握手协议（TLS Handshake）。较低的层为TLS记录协议，位于某个可靠的传输协议（例如TCP）上面。

　　TLS记录协议提供的连接安全性具有两个基本特性：

* 私有——对称加密用以数据加密（DES、RC4等）。对称加密所产生的密钥对每个连接都是唯一的，且此密钥基于另一个协议（如握手协议）协商。记录协议也可以不加密使用。
* 可靠——信息传输包括使用密钥的MAC进行信息完整性检查。安全哈希功能（SHA、MD5等）用于MAC计算。记录协议在没有MAC的情况下也能操作，但一般只能用于这种模式，即有另一个协议正在使用记录协议传输协商安全参数。

　　TLS记录协议用于封装各种高层协议。作为这种封装协议之一的握手协议允许服务器与客户机在应用程序协议传输和接收其第一个数据字节前彼此之间互相认证，协商加密算法和加密密钥。TLS握手协议提供的连接安全具有三个基本属性：

* 可以使用非对称的，或公共密钥的密码术来认证对等方的身份。该认证是可选的，但至少需要一个结点方。
* 共享解密密钥的协商是安全的。对偷窃者来说协商加密是难以获得的。此外经过认证过的连接不能获得加密，即使是进入连接中间的攻击者也不能。
* 协商是可靠的。没有经过通信方成员的检测，任何攻击者都不能修改通信协商。

　　TLS的最大优势就在于：TLS是独立于应用协议。高层协议可以透明地分布在TLS协议上面。然而，TLS标准并没有规定应用程序如何在TLS上增加安全性；它如何启动TLS握手协议以及如何解释交换的认证证书的决定权留给协议的设计者和实施者来判断。

　　协议结构

　　TLS协议包括两个协议组——TLS记录协议和TLS握手协议。

　　TLS和SSL的关系：并列关系

　　最新版本的TLS（Transport Layer Security，传输层安全协议）是IETF（Internet Engineering Task Force，Internet工程任务组）制定的一种新的协议，它建立在SSL 3.0协议规范之上，是SSL 3.0的后续版本。在TLS与SSL 3.0之间存在着显著的差别，主要是它们所支持的加密算法不同，所以TLS与SSL 3.0不能互操作。

　　1.TLS与SSL的差异

　　1）版本号：TLS记录格式与SSL记录格式相同，但版本号的值不同，TLS的版本1.0使用的版本号为SSLv3.1。

　　2）报文鉴别码：SSLv3.0和TLS的MAC算法及MAC计算的范围不同。TLS使用RFC-2104定义的HMAC算法。SSLv3.0使用了相似的算法，两者差别在于SSLv3.0中，填充字节与密钥之间采用的是连接运算，而HMAC算法采用的异或运算。但是两者的安全程度是相同的。

　　3）伪随机函数：TLS使用了称为PRF的伪随机函数来将密钥扩展成数据块，是更安全的方式。

　　4）报警代码：TLS支持几乎所有的SSLv3.0报警代码，而且TLS还补充定义了很多报警代码，如解密失败（decryption\_failed）、记录溢出（record\_overflow）、未知CA（unknown\_ca）、拒绝访问（access\_denied）等。

　　5）密文族和客户证书：SSLv3.0和TLS存在少量差别，即TLS不支持Fortezza密钥交换、加密算法和客户证书。

　　6）certificate\_verify和finished消息：SSLv3.0和TLS在用certificate\_verify和finished消息计算MD5和SHA-1散列码时，计算的输入有少许差别，但安全性相当。

　　7）加密计算：TLS和SSLv3.0在计算主密值（master secret）时采用的方式不同。

　　8）填充：用户数据加密之前需要增加的填充字节。在SSL中，填充后的数据长度哟啊达到密文快长度的最小整数倍。而在TLS中，填充后的数据长度可以是密文块长度的任意整数倍（但填充的最大长度为255字节），这种方式可以防止基于对报文长度进行分析的攻击。

　　2.TLS的主要增强内容

　　TLS的主要目标是使SSL更安全，并使协议的规范更精确和完善。TLS在SSL v3.0的基础上，提供了以下增加内容：

　　1）更安全的MAC算法

　　2）更严密的警报

　　3）“灰色区域”规范的更明确的定义

　　3.TLS对于安全性的改进

　　1）对于消息认证使用密钥散列法：TLS使用“消息认证代码的密钥散列法”（HMAC），当记录在开放的网络（如因特网）上传送时，该代码确保记录不会被变更。SSLv3.0还提供键控消息认证，但HMAC比SSLv3.0使用（消息认证代码）MAC功能更安全。

　　2）增强的伪随机功能（PRF）：PRF生成密钥数据。在TLS中，HMAC定义PRF。PRF使用两种散列算法保证其安全性。如果任一算法暴露了，只要第二种算法未暴露，则数据仍然是安全的。

　　3）改进的已完成消息验证：TLS和SSLv3.0都对两个端点提供已完成的消息，该消息认证交换的消息没有被变更。然而，TLS将此已完成消息基于PRF和HMAC值之上，这也比SSLv3.0更安全。

　　4）一致证书处理：与SSLv3.0不同，TLS试图指定必须在TLS之间实现交换的证书类型。

　　5）特定警报消息：TLS提供更多的特定和附加警报，以指示任一会话端点检测到的问题。TLS还对何时应该发送某些警报进行记录。

**[更多详细地介绍]**

1、聊聊HTTPS和SSL/TLS协议 | 程序师 - 程序员、编程语言、软件开发、编程技术 http://www.techug.com/post/https-ssl-tls.html

2、详解SSL/TLS http://www.mamicode.com/info-detail-1846390.html （推荐阅读）