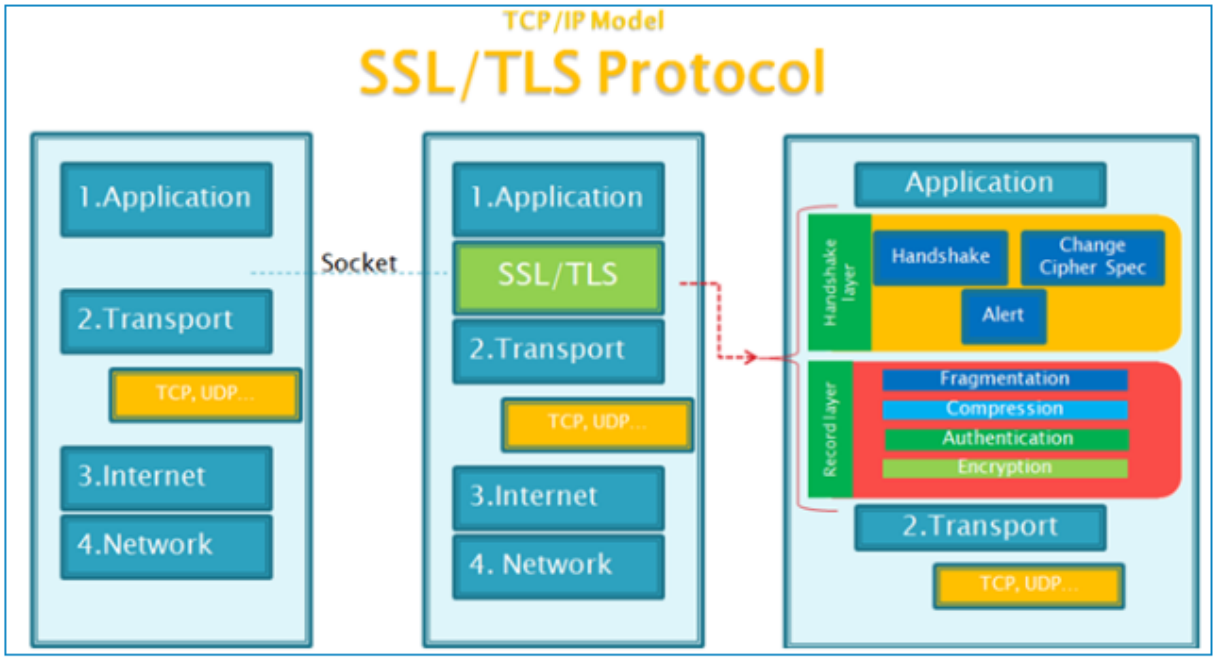

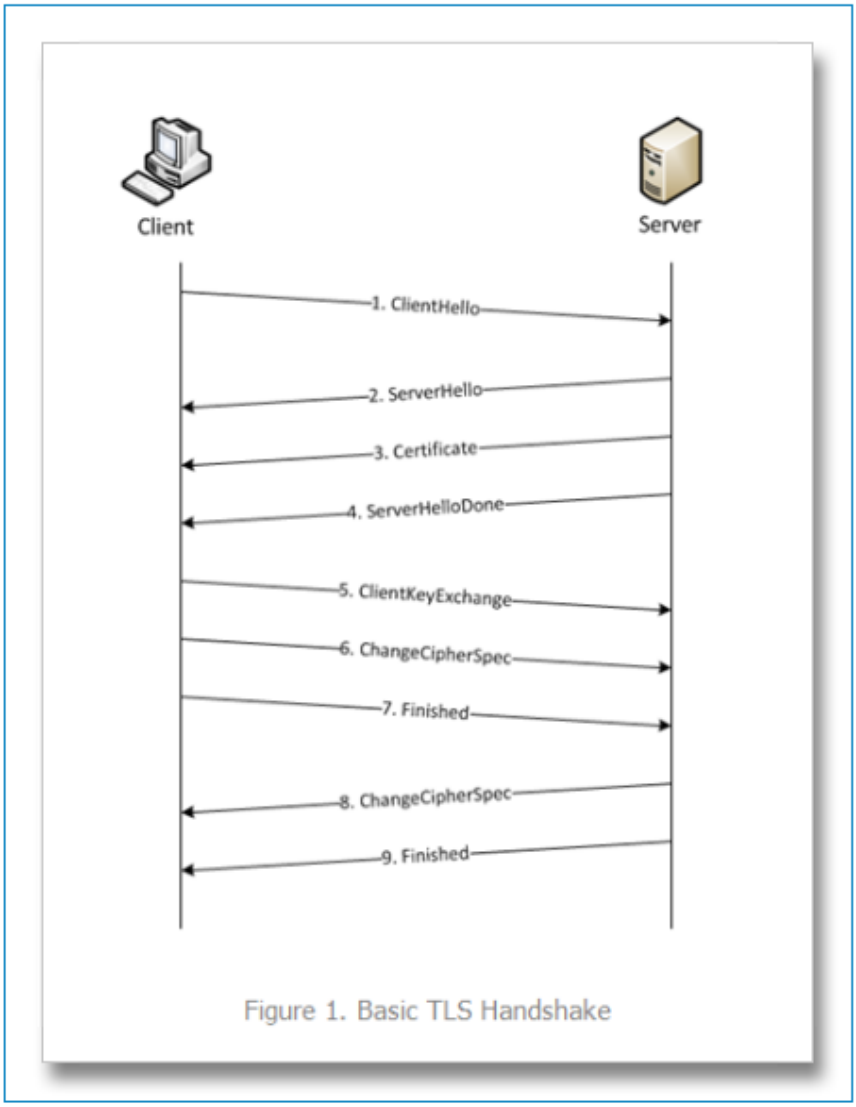

Figure 1. Basic TLS Handshake

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。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 secrity，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开发的专门用来保护web通讯的，而TLS是基于SSL以上的。

SSL:
为netscape所开发，用以保障在Internet上数据传输的安全，利用数据加密技术，可确保数据在网络上的传输过程中不会被截取。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，它建立在可靠的传输协议之上，为高层协议提供数据封装、压缩、加密等基本功能支持。SSL握手协议，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：
服务器认证服务：
1.客户端向服务器发送一个开始消息“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.客户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消息，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，客户则返回签名后的提问和其公开密钥，从而向服务器提供认证。

TSL协议：安全传输层协议

安全传输层协议（TSL）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记录协议和TLS握手协议。较低的层为TLS记录协议，位于某个可靠的传输协议上面。

TSL记录协议提供的连接安全性具有两个基本特征：

- 私有一对称加密用以数据加密。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
- 可靠的信息传输包括使用密钥的MAC进行信息完整性检查。安全哈希功能用户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相互认证，协商加密算法和加密密钥。TSL握手协议提供的连接安全具有三个基本属性：

1.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。

2.共享加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。即使进入连接中间的攻击者也不能。

3.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是独立于应用层协议。高层协议可以透明地分布在TLS协议上面。然而，TLS标准并没有规定如何在TSL上增加安全性。它把如何启动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。

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SSL3.0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SSL3.0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使用了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算法采用的是异或运算。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与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，填充后的数据长度要达到密文块长度的最小整数倍。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，提供了以下增强内容：

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使用的（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。