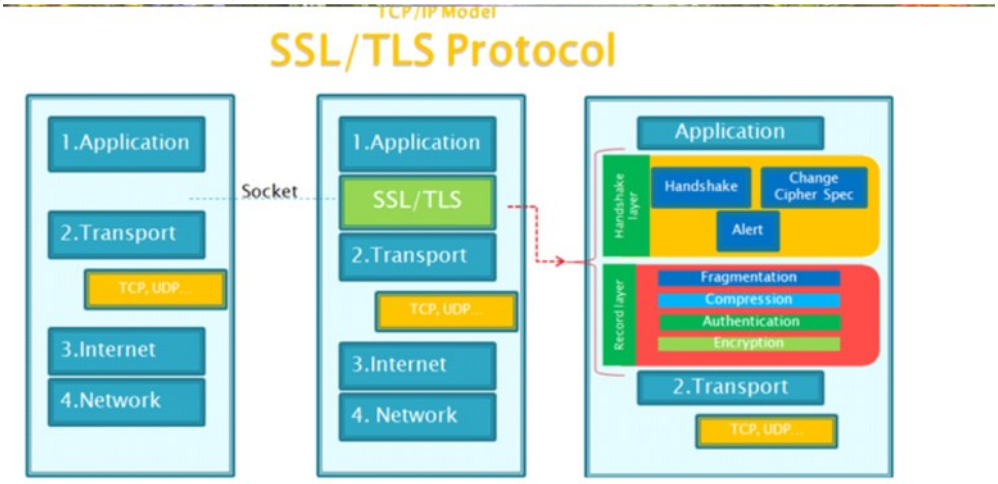
SSL/TSL原理

2018年6月24日 22:45

SSL介于HTTP和TCP之间的可选层



- SSL：（Secure Socket Layer，安全套接字层），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。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。

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。TLS 1.0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，可以理解为SSL 3.1。该协议由两层组成：TLS 记录协议（TLS Record）和 TLS 握手协议（TLS Handshake）。

SSL/TLS协议提供的服务：
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；
加密数据以防止数据中途被窃取；
维护数据的完整性，确保数据在传输过程中不被改变。

SSL双向认证具体过程
- 浏览器发送一个连接请求给安全服务器。
- 服务器将自己的证书，以及同证书相关的信息发送给客户浏览器。
- 客户浏览器检查服务器送过来的证书是否是由自己信赖的CA中心所签发的。如果是，就继续执行协议；如果不是，客户浏览器就给客户一个警告消息：警告客户这个证书不是可以信赖的，询问客户是否需要继续。
- 接着客户浏览器比较证书里的消息，例如域名和公钥，与服务器刚刚发送的相关消息是否一致，如果是一致的，客户浏览器认可这个服务器的合法身份。
- 服务器要求客户发送客户自己的证书。收到后，服务器验证客户的证书，如果没有通过验证，拒绝连接;如果通过验证，服务器获得用户的公钥。
- 客户浏览器告诉服务器自己所能够支持的通讯对称密码方案。
- 服务器从客户发送过来的密码方案中，选择一种加密程度最高的密码方案，用客户的公钥加过密后通知浏览器。
- 浏览器针对这个密码方案，选择一个通话密钥，接着用服务器的公钥加过密后发送给服务器。
- 服务器接收到浏览器送过来的消息，用自己的私钥解密，获得通话密钥。
- 服务器、浏览器接下来的通讯都是用对称密码方案，对称密钥是加过密的。
  双向认证则是需要服务端与客户端提供身份认证，只能是服务端允许的客户能去访问，安全性相对较高一些。

SSL单向认证具体过程
- 客户端的浏览器向服务器传送客户端SSL协议的版本号，加密算法的种类，产生的随机数，以及其他服务器和客户端之间通讯所需要的各种信息。
- 服务器向客户端传送SSL协议的版本号，加密算法的种类，随机数以及其他相关信息，同时服务器还将向客户端传送自己的证书。
- 客户利用服务器传过来的信息验证服务器的合法性。
- 用户端随机产生一个用于后面通讯的"对称密码"，然后用服务器的公钥)对其加密，然后将加密后的"对称密码"传给服务器。
- 服务器和客户端用相同的主密码即"对称密码"，对称密钥用于SSL协议的安全数据通讯的加解密通讯。同时在SSL通讯过程中还要完成数据通讯的完整性，防止数据通讯中的任何变化。
- SSL 单向认证只要求站点部署了 SSL 证书就行，任何用户都可以去访问，只是服务端提供了身份认证。

SSL双向认证和SSL单向认证的区别：双向认证 SSL 协议要求服务器和用户双方都有证书。单向认证 SSL 协议不需要客户拥有证书。单向认证的具体过程相对应于上面的步骤，只需将服务器端验证客户证书的过程去掉。一般 Web 应用配置 SSL 单向认证即可。但部分金融行业用户的应用对接，可能会要求对客户端做身份验证。这时就需要做 SSL 双向认证。