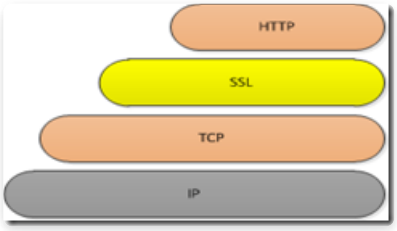
双向认证与单向认证

SSL 单向认证 双向认证

基本概念

- SSL / TLS
  SSL（ Secure Sockets Layer ），安全套接层。其继任者 TLS（ Transport Layer Security ）传输安全层 ，是为网络通信提供安全及数据完整性的一种安全协议。TLS与SSL在**传输层**对网络进行加密。

- HTTPS
  HTTPS（ Hypertext Transfer Protocol Secure ）安全超文本传输协议。
  HTTPS是以安全为目录的HTTP通道，简单讲是HTTP的安全版。即HTTP下加入SSL层。
  http协议直接放置在TCP协议之上，而https提出在http和TCP中间加上一层加密层。从发送端看，这一层负责把http的内容加密后送到下层 的TCP，从接收方看，这一层负责将TCP送来的数据解密还原成http的内容。
  所以https的协议栈应该如下图所示：



https 协议栈

- 数字证书

  一种文件的名称，好比一个机构或人的签名，能够证明这个机构或人的真实性。其中包含的信息，用于实现上述功能。

- 加密和认证

  加密是指通信双方为了防止铭感信息在信道上被第三方窃听而泄漏，将明文通过加密变成密文，如果第三方无法解密的话，就算他获得密文也无能为力；认证是指通信双方为了确认对方是值得信任的消息发送或接受方，而不是使用假身份的非法者，采取的确认身份的方式。只有同时进行了加密和认证才能保证通信的安全，因此在SSL通信协议中这两者都被应。早期一般是用对称加密算法，现在一般都是不对称加密，最常见的算法就是RSA。

- 消息摘要

  这个技术主要是为了避免消息被篡改。消息摘要是把一段信息，通过某种算法，得出一串字符串。这个字符串就是消息的摘要。如果消息被篡改（发生了变化），那么摘要也一定会发生变化（如果2个不同的消息生成的摘要是一样的，那么这就叫发生了碰撞）。

  消息摘要的算法主要有MD5和SHA，在证书领域，一般都是用SHA（安全哈希算法）。

- 单向认证
  客户端使用SSL时对服务端的证书进行认证，也就是说，客户端在请求建立之前，服务器会向客户端发送一

个证书，一般情况下，这种证书都是由企业自行发布的，所以在客户端使用HTTPS时，会跳出"是否信息并继续"，点击信任则表示客户端信息服务器端证书，才可以继续交互。

- 双向认证

  客户端和服务器端都对双方的证书进行验证，这时除了单向认证外，还需要在服务器端的受信任证书列表中加入客户端的证书，这样服务器才能信任客户端的请求。

认证过程

① 浏览器发送一个连接请求给安全服务器。

② 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。

③ 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。

④ 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。

⑤ 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。

⑥ 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。

⑦ 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。

⑧ 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。

⑨ 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。

⑩ 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。

上面所述的是双向认证 SSL 协议的具体通讯过程，这种情况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 CA 证书，具体的过程相对于上面的步骤，只需将服务器端验证客户证书的过程去掉，以及在协商对称密码方案，对称通话密钥时，服务器发送给客户的是没有加过密的（这并不影响 SSL 过程的安全性）密码方案。这样，双方具体的通讯内容，就是加过密的数据，如果有第三方攻击，获得的只是加密的数据，第三方要获得有用的信息，就需要对加密 的数据进行解密，这时候的安全就依赖于密码方案的安全。而幸运的是，目前所用的密码方案，只要通讯密钥长度足够的长，就足够的安全。这也是我们强调要求使用128 位加密通讯的原因。

参考文章

1. 百度百科
2. HTTPS单向认证和双向认证
3. https单向认证和双向认证