**HTTP与HTTPS握手的那些事**

**前提**

在讲述这两个握手时候，有一些东西需要提前说明。

**HTTP与TCP/IP区别？**

TPC/IP协议是传输层协议，主要解决数据如何在网络中传输，而HTTP是应用层协议，主要解决如何包装数据。WEB使用HTTP协议作应用层协议，以封装HTTP 文本信息，然后使用TCP/IP做传输层协议将它发到网络上。

下面的图表试图显示不同的TCP/IP和其他的协议在最初OSI（Open System Interconnect）模型中的位置：



PS：表格来自网上资料

**CA证书是什么？**

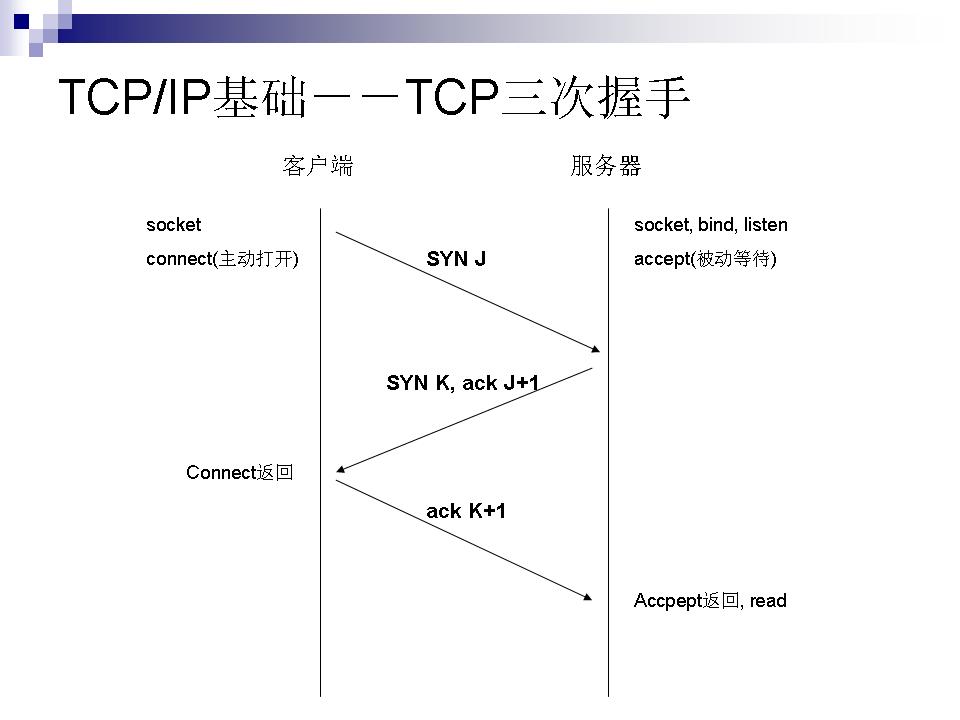
CA（Certificate Authority）是负责管理和签发证书的第三方权威机构，是所有行业和公众都信任的、认可的。

CA证书，就是CA颁发的证书，可用于验证网站是否可信（针对HTTPS）、验证某文件是否可信（是否被篡改）等，也可以用一个证书来证明另一个证书是真实可信，最顶级的证书称为根证书。除了根证书（自己证明自己是可靠），其它证书都要依靠上一级的证书，来证明自己。

**HTTP三次握手**

HTTP（HyperText Transfer Protocol)超文本传输协议是互联网上应用最为广泛的一种网络协议。由于信息是明文传输，所以被认为是不安全的。而关于HTTP的三次握手，其实就是使用三次TCP握手确认建立一个HTTP连接。

如下图所示，SYN（synchronous）是TCP/IP建立连接时使用的握手信号、Sequence number（序列号）、Acknowledge number（确认号码），三个箭头指向就代表三次握手，完成三次握手，客户端与服务器开始传送数据。



PS：图片来自网上资料

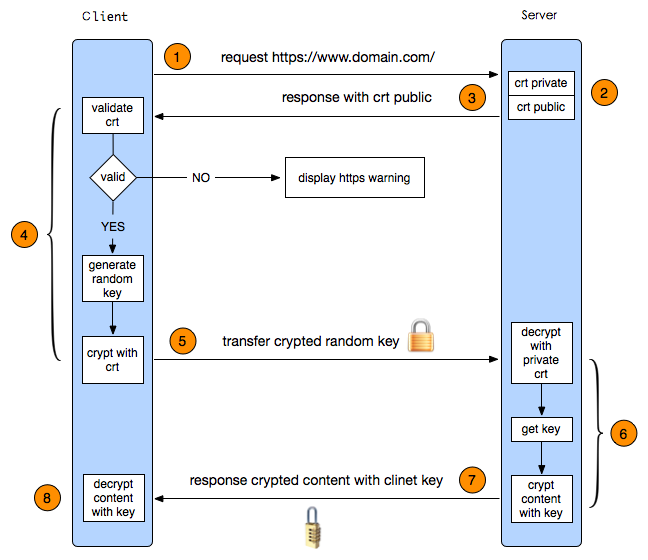
第一次握手：客户端发送syn包(syn=j)到服务器，并进入SYN\_SEND状态，等待服务器确认；

第二次握手：服务器收到syn包，必须确认客户的SYN（ack=j+1），同时自己也发送一个SYN包（syn=k），即SYN+ACK包，此时服务器进入SYN\_RECV状态；

第三次握手：客户端收到服务器的SYN＋ACK包，向服务器发送确认包ACK(ack=k+1)，此包发送完毕，客户端和服务器进入ESTABLISHED状态，完成三次握手。

**HTTPS握手过程**

HTTPS在HTTP的基础上加入了SSL协议，SSL依靠证书来验证服务器的身份，并为浏览器和服务器之间的通信加密。具体是如何进行加密，解密，验证的，且看下图，下面的称为一次握手。



PS：图片以下描述摘自：http://zhuqil.cnblogs.com

1. 客户端发起HTTPS请求

2. 服务端的配置

采用HTTPS协议的服务器必须要有一套数字证书，可以是自己制作或者CA证书。区别就是自己颁发的证书需要客户端验证通过，才可以继续访问，而使用CA证书则不会弹出提示页面。这套证书其实就是一对公钥和私钥。公钥给别人加密使用，私钥给自己解密使用。

3. 传送证书

这个证书其实就是公钥，只是包含了很多信息，如证书的颁发机构，过期时间等。

4. 客户端解析证书

这部分工作是有客户端的TLS来完成的，首先会验证公钥是否有效，比如颁发机构，过期时间等，如果发现异常，则会弹出一个警告框，提示证书存在问题。如果证书没有问题，那么就生成一个随即值，然后用证书对该随机值进行加密。

5. 传送加密信息

这部分传送的是用证书加密后的随机值，目的就是让服务端得到这个随机值，以后客户端和服务端的通信就可以通过这个随机值来进行加密解密了。

6. 服务段解密信息

服务端用私钥解密后，得到了客户端传过来的随机值(私钥)，然后把内容通过该值进行对称加密。所谓对称加密就是，将信息和私钥通过某种算法混合在一起，这样除非知道私钥，不然无法获取内容，而正好客户端和服务端都知道这个私钥，所以只要加密算法够彪悍，私钥够复杂，数据就够安全。

7. 传输加密后的信息

这部分信息是服务段用私钥加密后的信息，可以在客户端被还原。

8. 客户端解密信息

客户端用之前生成的私钥解密服务段传过来的信息，于是获取了解密后的内容。

PS: 整个握手过程第三方即使监听到了数据，也束手无策。

**总结**

为什么HTTPS是安全的？

在HTTPS握手的第四步中，如果站点的证书是不受信任的，会显示出现下面确认界面，确认了网站的真实性。另外第六和八步，使用客户端私钥加密解密，保证了数据传输的安全。



**HTTPS和HTTP的区别**

1. https协议需要到ca申请证书或自制证书。

2. http的信息是明文传输，https则是具有安全性的ssl加密。

3. http是直接与TCP进行数据传输，而https是经过一层SSL（OSI表示层），用的端口也不一样，前者是80（需要国内备案），后者是443。

4. http的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比http协议安全。

**注意https加密是在传输层**

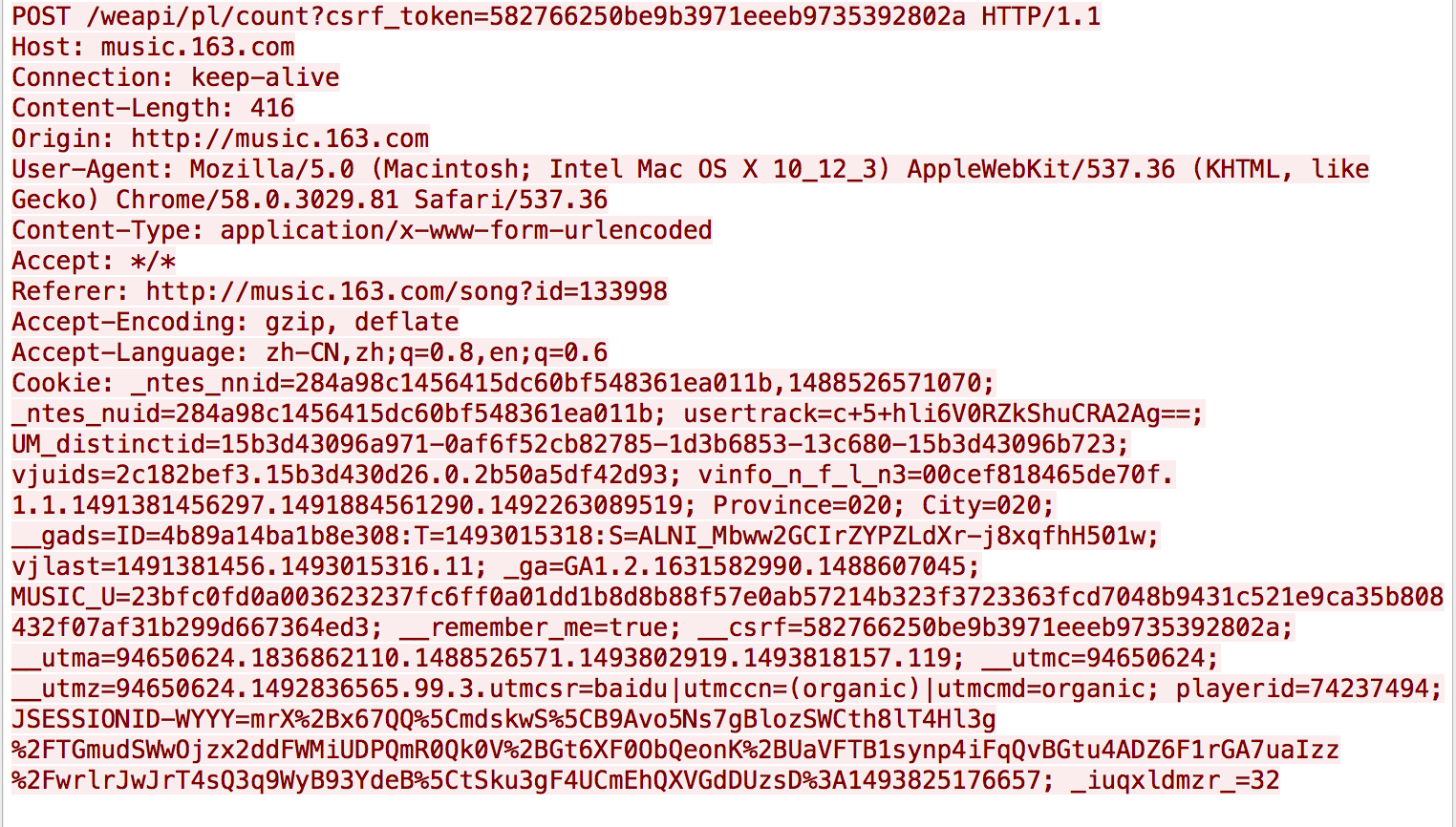
https报文在被包装成tcp报文的时候完成加密的过程，无论是https的header域也好，body域也罢都是会被加密的。

当使用tcpdump或者wireshark之类的tcp层工具抓包，获取是加密的内容，而如果用应用层抓包，使用Charels(Mac)、Fildder(Windows)抓包工具，那当然看到是明文的。

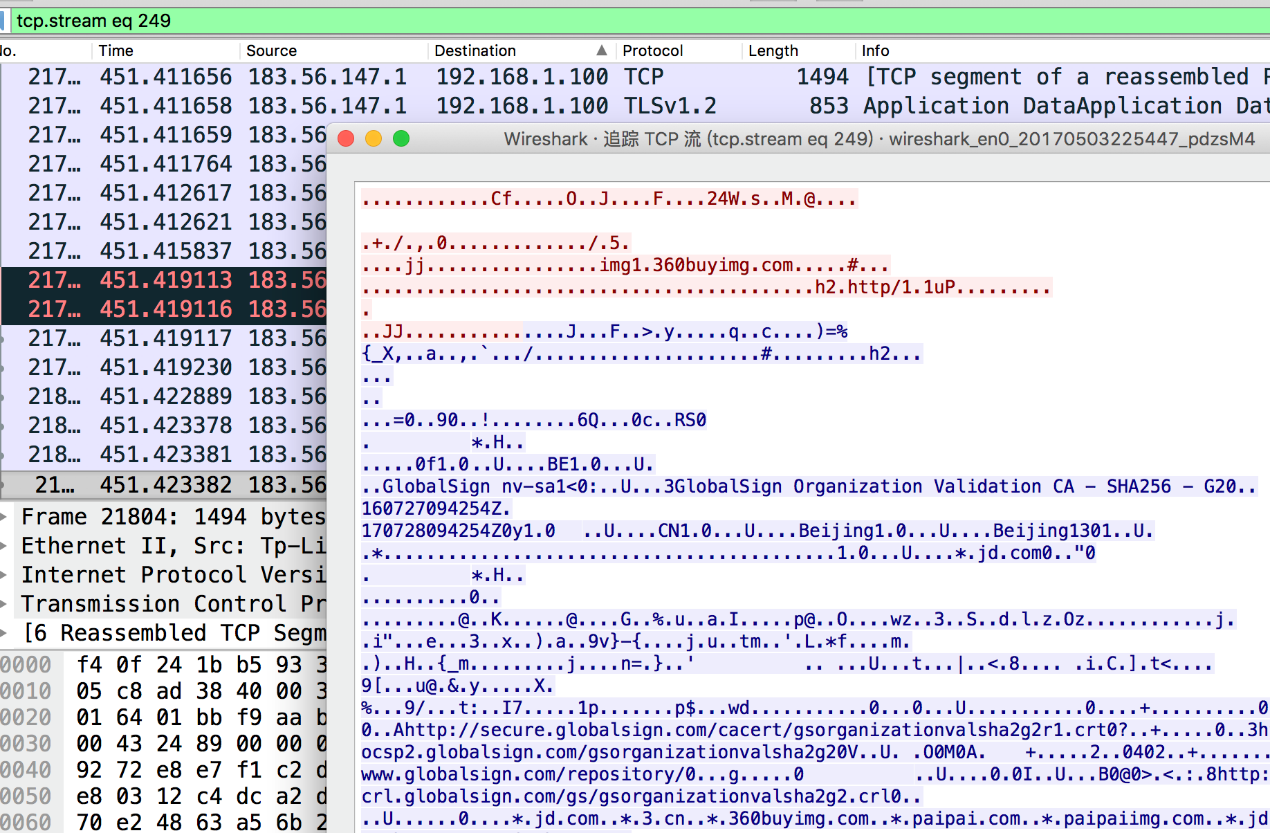
PS：HTTPS本身就是为了网络的传输安全。

例子，使用wireshark抓包：

http，可以看到抓到是明文的：



https，可以看到抓到是密文的：



附录

HTTPS一般使用的加密与HASH算法如下：

非对称加密算法：RSA，DSA/DSS

对称加密算法：AES，RC4，3DES

HASH算法：MD5，SHA1，SHA256