<https://blog.csdn.net/woshinannan741/article/details/71550436>

# 搞懂HTTPS的过程和原理

2017年05月10日 16:50:15 [Helios\_nannan](https://me.csdn.net/woshinannan741) 阅读数：4848更多

个人分类： [http协议](https://blog.csdn.net/woshinannan741/article/category/6911195)

版权声明：本文为博主原创文章，转载请注明出处 https://blog.csdn.net/woshinannan741/article/details/71550436

最近想重构自己的个人网站+升级到http/2顺便学习一些新的知识。   
如果想升级到http/2那么就要先吧网站升级到https,这是因为在现在这个阶段所有的浏览器都只支持HTTP/2 Over TLS,也就是说浏览器中的http/2必须基于HTTPS的部署。

## 什么是https

因为一般的http协议是明文传输的，是不会进行保密的，因此使用http协议传送隐秘信息的时候是十分不安全的。所以网景公司就设计了SSL协议，最新的SSL的版本是3.03.0，关于TLS就是SSL的升级版本。现在我们使用的https协议都是用的是TLS协议，由于SSL被大多数的浏览器支持，因此SSL依旧是https的代名词。如果想对SSL/TLS有更深一步了解，请异步[SSL/TLS的wiki](https://en.wikipedia.org/wiki/Transport_Layer_Security)

## https是不是绝对安全

这个的答案是否定的，HTTPS只是解决了数据在传输过程中的安全性和保密性,这一点用一般的wireshark就能验证(注意这里指的是一般)。如果是服务器或者证书出现问题那么https是肯定解决不了的。

## HTTPS的原理

### 先来说说对称加密和非对称加密

#### 对称加密

就是通信的双方使用的是同一套算法，比如说对一个文件进行用这个算法进行加密，那么用这个算法或者这个算法的逆过程就能解密，这样带来的开销往往会小一些

#### 非对称加密

为什么会出现非对称加密，就是因为对称加密的算法是可以被攻破的，(最坏的情况下穷举攻击能攻破的)，就比如说当初密码学刚刚产生的时候的凯撒密码，如下：

abcd

* 1

进行加密之后变为：

efgh

* 1

我们很容易就能够猜出来就是由明文的每个字符+4就变成了密文，这样如果算法被攻破的话，密码也就随之知道了。

非对称加密分为两个密钥：公钥和私钥。公钥是谁都能有，用于对信息加密，只有私钥才能解密。如果想进一步了解，可以看看我以前写过的一篇关于RSA的的文章(要有一定的数论基础哟)：[RSA非堆成加密算法的实现](http://blog.csdn.net/woshinannan741/article/details/52790511)

如果您了解了非对称加密算法，就知道这个算法相对于对称加密算法来说，是十分浪费时间和资源的

### https要知道的几个加密算法

1. 握手的时候使用的非对称加密算法 ，用来加密握手之后的请求和应答
2. 传输信息的时候使用的对称加密，
3. 保证数据的完整性用的是hash算法(数字签名)

### 为什么要有https

我们来假设几个场景：

1. A(浏览器)和B(服务器)发送隐私的信息 ( http是明文传输怎么搞？
2. 就算加密了，攻击者C获得了双方加密的密钥，也能获得双方的信息呀 ( 密钥丢失了怎么办呀？
3. 就算攻击者C没有办法获得密钥，那么C向B(服务器)发送一些数据，那么B也不知道是不是A发送的呀 (　A是不是A？

### HTPS的工作过程

1. 客户端发送自己支持的加密规则给服务器，代表告诉服务器要进行连接了
2. 服务器从中选出一套加密算法和hash算法以及自己的身份信息(地址等)以证书的形式发送给浏览器，证书中包含服务器信息，加密公钥，证书的办法机构
3. 客户端收到网站的证书之后要做下面的事情：   
   * 验证证书的合法性
   * 如果验证通过证书，浏览器会生成一串随机数，并用证书中的公钥进行加密
   * 用约定好的hash算法计算握手消息，然后用生成的密钥进行加密，然后一起发送给服务器
4. 服务器接收到客户端传送来的信息，要求下面的事情：   
   * 用私钥解析出密码，，用密码解析握手消息，验证hash值是否和浏览器发来的一致
   * 使用密钥加密消息，回送
5. 如果计算法hash值一致，握手成功

其他https好的文章 ：   
- [HTTPS原理](http://www.guokr.com/post/114121/)   
- [看完还不懂HTTPS我直播吃翔](http://qifuguang.me/2017/03/25/%E7%9C%8B%E5%AE%8C%E8%BF%98%E4%B8%8D%E6%87%82HTTPS%E6%88%91%E7%9B%B4%E6%92%AD%E5%90%83%E7%BF%94/)