浅析 HTTPS 协议的原理及应用

◆张宝玉

（菏泽家政职业学院　山东　274300）

摘要：本文详细阐述了 Https 协议的工作原理，并结合实际应用情况，对 Https 协议的应用前景进行了展望。
关键词：HTTPS；网络协议；SSL 协议

0　引言

2015 年 3 月，百度公司推出全站 Https 安全加密服务，对传统 Http 通道添加 SSL 安全套接层，将用户的搜索请求全部变成加密状态，旨在为广大网民提供更加安全、私密的信息服务。同年 10 月，阿里巴巴宣布旗下所有电商平台实现全站 Https，京东、亚马逊也在登录或交易页面启用了 Https。细心的网友可能会发现，国内几大银行网站域名前缀为“http://”，而进行网上银行交易时域名前缀自动变为“https://”。

从 Http 到 Https，百度投入了数千台服务器，上亿元的成本。不仅仅是资金投入，技术难度和工作量也相当大，从搜索基础架构调试，到全部域名（主域名和子域名）的修改，再到速度的优化，并解决了中间者劫持问题，百度公司半年来投入的程序员、工程师加起来有上百人，相当于把整个搜索的元素进行了 Https 的改写。花销这么大的人力、物力、财力，还冒着相当大的风险，百度公司为何这般重视 Https？Https 到底有什么作用，发展趋势如何？

1　概念

我们先了解几个相关关键词的概念和含义：

1.1　HTTP 协议

超文本传输协议（Hypertext transfer protocol），它约定了浏览器和万维网服务器之间通信的规则，是应用最广泛的网上传输数据的基础协议，目前绝大多数的网站都采用 Http 协议。但是 Http 采用的是明文传送，消息完整性检测也不充分。这种安全缺陷很容易被利用以获取网民的信息，如访问记录、账号、密码等。尤其是当前网上交易、网上支付已非常普遍，其安全弊端越来越突出。

1.2　SSL 协议

SSL（Secure Sockets Layer 安全套接层，其继任者为 TLS）是为网络通信提供安全及数据完整性的一种安全协议。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传输的过程中不会被截取及窃听。

1.3　HTTPS 协议

安全超文本传输协议（Hypertext Transfer Protocol Secure），是由 HTTP + SSL 协议构建的可进行加密传输、身份认证的网络协议，在 Http 的基础上通过传输加密和身份认证保证了传输过程中的安全性，比 Http 协议更加安全。最直观的特征是以 https:// 开头并且地址栏两端有小锁样式的图标。图 1 所示为 Google chrome、Firefox、IE10 在使用 Https 时的效果：

图 1　使用 Https 时的效果

HTTPS 协议特点：

（1）Https 需要到 CA 申请证书，一般是收费的；

（2）Http 是超文本传输协议，信息是明文传输，Https 则是具有安全性的 SSL 加密传输协议；

（3）Http 一般使用的端口是 80 端口，Https 一般使用 443 端口。

1.4　SSL 证书

也称为服务器 SSL 证书，是遵守 SSL 协议的一种数字证书，由全球信任的证书颁发机构（CA）验证服务器身份后颁发。证书就是一种网络上证明持有者身份的文件，同时证书中还含有公钥。通常 Windows 部署系统的时候会在客户机上安装“根受信任机构列表”，当客户端收到一个证书时会核对证书是否为列表中的机构颁发的，如果是则信任这个证书。

2　SSL 协议原理

2.1　SSL 的位置

SSL 协议位于应用层和 TCP 层之间。应用层数据不再直接传递给传输层，而是传递给 SSL 层，SSL 层把从应用层收到的数据进行加密，并增加自己的 SSL 头。

2.2　SSL 的工作原理

SSL 协议由三部分组成：握手协议，记录协议，警报协议。

（1）握手协议（Handshake protocol）

握手协议是客户端和服务器端用 SSL 连接通信时首先使用的协议，包括客户机与服务器之间的一系列消息。该协议允许客户机和服务器相互验证，协商加密和 MAC 算法以及保密密钥。握手协议是在应用程序的数据传输之前使用的。握手协议过程可分为四个阶段，如图 2 所示：

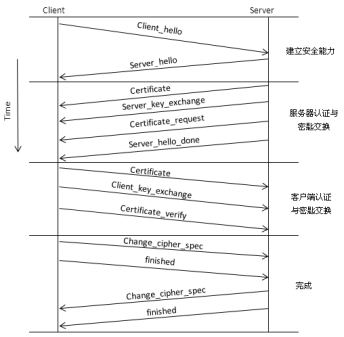

图 2　握手协议过程

①建立安全能力

这个阶段主要是启动逻辑连接，建立连接的安全功能。客户端先向服务器端送出一个 client hello 消息，服务器向客户机返回 server hello 消息，并对 client hello 消息中的信息进行确认。

②服务器认证与密钥交换

当服务器送出 server hello 消息后，或客户端需要验证服务器的身份时，服务器将其证书资料传送给客户端。

③客户机认证与密钥交换

当收到服务器送出的 server done 消息后，客户机核对服务器提供的证书是否正确，接着再确认 server done 消息中所携带的参数是否能够接受。如果这些都能满足的话，客户机会响应一个或多个消息给服务器。

④完成

客户机送出 change cipher spec 消息，将密码套件状态更新为将要使用的密码套件状态。紧接着，客户机利用之前与服务器协议得到的算法、密钥，来传送最后的 finished 消息，用来证明密钥交换以及认证的过程已经完成。为了响应这两个消息，服务器会传送自己的 change cipher spec 消息，并将密码套件状态更新为

将要使用密码套件状态，最后再送出 finished 消息。当这些步骤完成后，客户端与服务器就能开始传送应用层的数据了。

（2）记录协议（Record protocol）

当客户机和服务器鉴别对方并确定安全信息交换使用的算法后，进入 SSL 记录协议，记录协议提供两个服务：

①数据保密性：使用握手协议定义的秘密密钥对 SSL 所传送的数据加密。

②消息完整性：使用握手协议定义的带有 MAC 的密钥计算出消息认证码。

SSL 记录协议操作流程如图 3 所示：

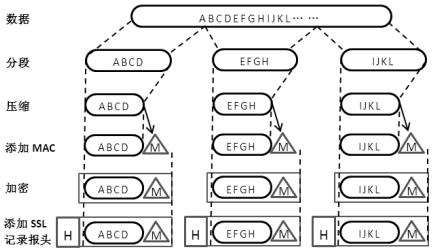

图 3　SSL 记录协议操作流程

记录协议接收到应用程序传送的消息，将数据分片（切成容易管理的小区块），然后选择是否对这些区块作压缩，再加上此区块的消息认证码。接着将数据区块与 MAC 一起做加密处理，加上 SSL 记录头后通过 TCP 传送出去。接收数据的那一方对数据进行解释、核查、解压缩、重组，将消息的内容还原，传送给上层使用者。

（3）警报协议（Alert protocol）

当客户机和服务器发现错误时，会向对方发送一个警报消息。如果是致命错误，算法立即终止会话并关闭 SSL 连接，同时还会删除相关的会话记录、秘密和密钥。

总之，在 SSL 工作过程中，使用握手协议协商加密和 MAC 算法以及保密密钥，使用记录协议对交换的数据进行加密和签名，使用警报协议解决出现的问题。

3　SSL 证书的作用和验证过程

3.1　SSL 证书的作用

（1）认证服务器。网站部署全球信任的 SSL 证书后，浏览器内置安全机制，实时查验证书状态，通过浏览器向用户展示网站认证信息，让用户轻松识别网站真实身份，防止钓鱼网站仿冒。

（2）实现加密传输。安装 SSL 证书后，使用 Https 加密协议访问网站，可激活客户端浏览器到网站服务器之间的"SSL 加密通道"（SSL 协议），实现高强度双向加密传输，防止传输数据被泄露或篡改。

3.2　SSL 证书的颁发和验证过程

Ssl 证书颁发和验证过程如图 4 所示：

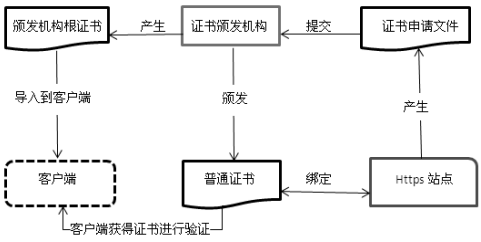

图 4　证书颁发和验证过程

浏览器会从如下三个方面验证证书的有效性，不满足情况下会报警提示：

（1）证书颁发者是否在“根受信任的证书颁发机构列表”中；

（2）证书是否过期；

（3）证书的持有者是否和访问的网站一致。

除此之外浏览器还会定期更新证书颁发者的“证书吊销列表”，如果某个证书虽然符合上述条件，但是被它的颁发者在“证书吊销列表”中列出，那么也将给出警告。

4　HTTPS 协议工作原理

4.1　HTTPS 协议的工作流程

HTTPS 在真正的数据交互之前通过 SSL 握手协议协商一个对称密钥，通过这个对称密钥对以后的通信数据进行加密。其通信过程如图 5 所示：

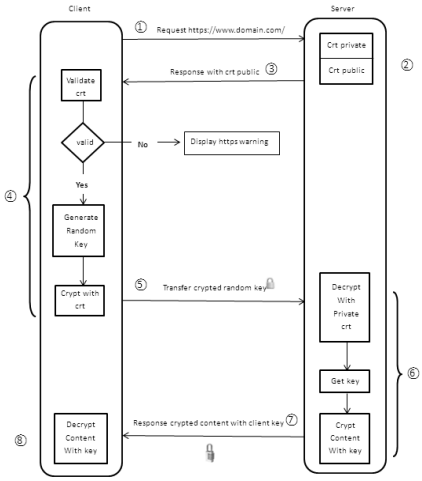

图 5　HTTPS 协议的工作流程

（1）客户端发起 HTTPS 请求

用户在浏览器里输入 Https 网址，然后连接到 server 的 443 端口。

（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，可以自己制作，也可以向组织申请。两者的区别就是自己颁发的证书需要通过客户端验证后才可以继续访问，而使用受信任的公司申请的证书则不会弹出提示页面。数字证书其实就是一对公钥和私钥，就好比一个锁和一把钥匙，并且只有你自己有这把钥匙，把锁交给别人，别人把重要的东西锁起后发给你，因为只有你有这把钥匙，所以也只有你才能看到被这把锁锁起来的东西。

（3）传送证书

这个证书就是公钥。

（4）客户端解析证书

SSL 首先验证收到的公钥是否有效，比如颁发机构、过期时间等，如果发现异常，弹出警告框，提示证书存在问题，不然，就生成一个随即值，接着用证书对该随机值进行加密。正如前面讲的，把随机值用锁头锁起来，这样除非有钥匙，锁住的内容是不会被看到的。

（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（第二个私钥），然后把数据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

这部分信息是服务器端用私钥（第二个私钥）加密后的信息，可以在客户端被还原

（8）客户端解密信息

客户端用前面生成的私钥（第二个私钥）解密从服务器端传送过来的信息，于是获取了解密后的内容。整个过程第三方即使监听到了数据，也束手无策。

4.2　HTTPS 协议的加密方法

加密算法分为两种：对称加密和非对称加密。所谓对称加密（也叫密钥加密）就是指加密和解密使用的是相同的密钥。而非对称加密（也叫公钥加密）就是指加密和解密使用了不同的密钥。

（下转第 39 页）

并没有在 P2P 网络被剔除。并且，在 P2P 网络中存在着一种自私节点，它们的存在降低了 P2P 文件共享系统的网络利用率，打破了共享资源的平衡。根据研究，大约有 70%的网络节点没有向他人分享过资源，而是仅仅 1%的节点提供的资源在资源总量中占了 50%。P2P 文件共享系统中这些恶意节点和自私节点的存在会拖累其发展的速度，降低网络的利用率，所以，必须建立相应的机制来抑制恶意节点和自私节点的发展。正因为如此，要在 P2P 网络中应用双向信任机制，用于遏制恶意节点和自私节点的产生和发展，提高网络的利用率，增加各个节点的信任度。

3.3　双向信任机制的信任度计算方法

双向信任机制的信任度的计算方法主要分为对提供节点信任度和请求节点信任度的计算，用于在文件共享时节点之间信任关系的双向评估。提供节点信任度是针对于提供节点所提供的服务的可信性，请求节点信任度则是表明了请求节点的资源访问权限。服务信任度是请求节点在选择提供节点时的一个标准，与请求节点的请求信任度并没有丝毫的关系，而请求节点的请求信任度只是在提供节点收到服务请求时，才会成为一个标准。

假设节点 A 作为一个请求节点，而节点 B 的服务信任度大于 Threshhold A，节点 A 将节点 B 作为提供节点，节点 A 将会向节点 B 发出请求服务的要求；但是，如果节点 B 的服务信任度小于 Threshhold A，节点 A 就不会选择节点 B 进行服务，而是重新寻找其他的节点提供服务。

节点 B 在收到节点 A 的请求服务的要求后，确认节点 A 资源共享请求的可信任度，参照其他的标准，给予节点 A 对共享资源的可访问权限。当节点 B 确认时，交易初始行为结束，正式开始进入交易阶段。

4　结语

综上所述，对等的节点之间的信任关系已经成为 P2P 网络中文件共享系统发展过程中亟待解决的重要问题。提高提供节点的可信度，一个可信的提供节点和一个可信任度高的请求节点可以提高交易过程中共享资源的安全性，促进交易行为的正常发展。类似于人与人之间关系网络，P2P 文件共享交易存在着相互信任的问题，所以，为提高节点的可信度建立一个公开、透明、有序的交易环境，在 P2P 网络中应用双向信任机制就显得尤为重要。双向信任机制可以提高整个网络的利用率，增加各个节点之间的信任度，保障资源共享时的公平性，保证服务质量。只有在 P2P 网络中应用双向信任机制，P2P 文件共享系统才会获得一个发展机会，消除恶意节点和自私节点带来的不良影响。

参考文献：

[1]陈国强，苏静.P2P 文件共享系统中的一种双向并发信任机制[J].微电子学与计算机，2011.

[2]李娟.P2P 网络中双向信任机制的研究[J].办公自动化，2011.

[3]宋晓飞.基于反馈评价的 P2P 网络信任机制探究[J].计算机光盘软件与应用，2015.

[4]王学龙，张璟.P2P 在制造资源信息共享中的应用[J].计算机工程与应用，2012.

[5]张玉洁，何明，孟祥武.基于用户需求的内容分发点对点网络系统研究[J].软件学报，2014.

[6]张伟楠.基于交易特征和反馈评价的 P2P 网络信任模型研究[D].江西理工大学，2013.

（上接第 37 页）

对称内容加密强度非常高，一般不会被破解。但是要安全地生成和保管密钥却是个很大的问题，如果客户端和服务器的会话都使用固定的密钥来加密和解密，而对称密钥又被其它人获取，整个数据交换就不安全了。

非对称加密主要用于密钥交换（也叫密钥协商），能够很好地解决这个问题。浏览器和服务器每次新建会话时都使用非对称密钥交换算法协商出对称密钥，使用这些对称密钥完成应用数据的加解密和验证，密钥只在内存中生成和保存，并且每次会话的对称密钥都不相同（除非会话重复使用），中间者是无法窃取的。

5　HTTPS 没有全面普及的原因

既然 HTTPS 协议这么安全，为什么没有更早地在互联网上全面普及呢？原因如下几点：

5.1　Https 与 Http 通信过程的差异

（1）302 重定向，如果用户没有在地址栏中直接输入前缀 Https://进行访问，就会出现重定向过程；

（2）SSL 握手过程增加了网络传输 RTT 和数字签名校验，很多移动终端本身计算性能就不是很强，耗时会更加明显；

（3）证书验证和状态检验。浏览器一般会通过 OCSP 来检查证书的撤销状态，在拿到服务器发送过来的证书之后会请求 OCSP 站点获取证书的状态，如果 OCSP 站点位于国外或者出现故障的话会影响这个正常用户的访问速度。

5.2　HTTPS 对访问速度有影响

HTTPS 协议交互增加了网络 RTT（round trip time）。协议握手阶段比较费时间，对网站的反应速度会产生负面的影响。同时，HTTPS 加密/解密也会产生计算耗时。要解决速度问题，通常会使用 SSL 加速器（专用服务器）来改善，需要增加硬件设备以分担负载提高速度。

5.3　SSL 证书需要交费

在 HTTPS 协议中，证书是必须的，使用证书必须向认证机构（CA）购买，功能越强大的证书费用会越高，因此，很多安全性要求不高的网站不愿多此费用支出。节约购买和维护证书的开销也是原因之一。

5.4　HTTPS 服务器端的负载增加

与明文通信相比，加密通信要消耗更多的 CPU 和内存资源，如果每次通信都加密，会消耗相当多的资源，访问量较多的网站需要增加投入更大的成本。因此，有些网站只是在传输包含敏感信息或保密数据时，才利用 HTTPS 加密通信，并非对所有内容都进行加密处理。

6　结语

国外的大型互联网公司很多已经启用了全站 HTTPS，这也是未来互联网发展的趋势。国内的大型互联网企业大多是在一些涉及账户或者交易的子页面 / 子请求上启用了 HTTPS。百度和阿里巴巴率先全站部署 HTTPS，对国内互联网行业的全站 HTTPS 进程必将有着巨大示范引领推动作用，随着 HTTPS 的不断的推广和普及，带给我们的将是一个更加安全的网络环境。

参考文献：

[1]黄河.编著.计算机网络安全——协议、技术与应用[M].清华大学出版社，2008.

[2]熊平.主编.信息安全原理及应用[M].清华大学出版社，2009.