朱旭东 （广东湛江海洋大学海滨学院 524005）

基于SSL的安全网站的理论与实践

The Theory and the Practice of Safe Web Site Based on SSL

摘要：Web服务器和客户机之间的传输数据的安全性一直是电子商务应用的重中之重。本文首先对SSL理论作深入解剖，然后以普遍使用的IIS 5.0 Web Server为例，避开复杂的编程，通过简单的操作具体实现SSL。

关键词：SSL RSA Web Server

1 引言

在Internet的快速发展过程中，通过Internet传输的数据的安全性一直是一个受高度关注的课题。由于互联网是一个完全开放的网络，使得在其上传输的各种数据都有面临种种被窃听和丢失的危险。如何做到既保证传输数据的安全，又方便实现，就成了网站开发建设者的头等大事。当前，多数国际知名企业都采用SSL加密机制来保证传输安全的安全。

2 SSL理论基础

SSL（Security Socket Layer）是一个用来保证安全传输文件的协议，SSL是Netscape公司开发的，当前版本为3.0，在套接口上工作。用于在服务器和客户机之间建立一条安全通道，从而实现在Internet中传输保密数据。很多SSL的功能也是Ipv6的一部分。

2.1 SSL的位置及组成

在TCP/IP协议族中，SSL位于TCP层之上，应用层之下。这使它可以独立于应用层，从而使应用层协议可以直接建立在SSL上。其大致位置如图1：

SSL协议由两部分组成：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，通信双方进行身份认证、协商加密算法、交换加密密钥等。

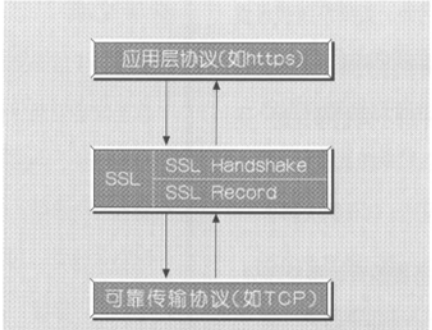

图1

2.2 SSL的实现流程

当一台计算机试图使用SSL建立连接时，要发生握手操作，SSL中有三类基本握手。SSL缺省只进行server端的认证，客户端的认证是可选的，即第一类握手。图2具体解释第一类握手，其余类似。

当客户机试图建立SSL连接时，发送CLIENT_HELLO消息给服务器，包括一个质疑、希望的连接或能够支持的加密体系。

服务器以SERVER_HELLO消息作为应答，包括连接标识、密钥证书以及服务器可以支持的加密体系。在两次出现的加密体系中，由客户机选择一种。

客户机检验服务器的公开密钥，并且向服务器发送CLIENT_MASTER_KEY消息，这是随机产生的主密钥，用服务器的公开密钥加密该主密钥后发送。可以看出，这里采用的公开密

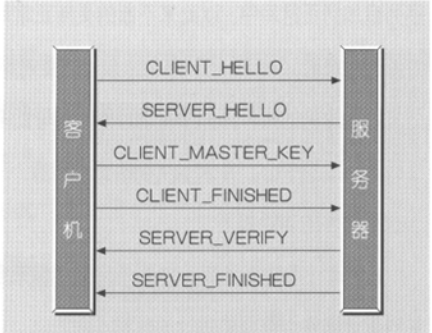

图2

钥密码体制，常用的有RSA等。然后客户机发送CLIENT_FINISHED消息，包括被客户写密钥加密的连接标识。

服务器发送SERVER_VERIFY消息，包括一个被服务器写密钥加密的客户机的质疑。

最后，服务器发送SERVER_FINISHED消息，包括一个被服务器写密钥加密的新的对话标识。

至此，一个安全的加密的服务器与客户机的通道已经建立起来，此后的传输数据都经过加密。

2.3 SSL的安全性及误区

SSL能实现数据的安全保密传输是指：通过SSL传输的数据是经过服务器与客户机的公开密钥密码体制加密，而且密钥是在传输开始时经协商随机产生的。这样即使在传输过程中数据被非法窃取，第三方没有解密密钥，也无法获得传输的原始数据或篡改原始数据。有关公开密码体制加密的安全性，请参见其他资料。典型的如MIT的RSA（Rivest,Shamir,Sdleman）是基于数论原理（Rivest等，1978）。

SSL保证的是传输过程中数据的安全保密，对网站服务器的安全没有提供特别的保证。在实践中，很多网络安全管理员由于对SSL的错误理解，对网站服务器的安全重视不够，使得SSL的实现成了无源之水，违背了网络安全的初衷。

3 SSL的实践

实现SSL的技术很多，采用编程的比较简单的有JSSE、JSP等方法。这里介绍一种不需要编程，直接配置的方法，采用的平台为：Windows 2000 Advanced Server，Web Server为IIS 5.0。采用Apache Web Server也可以方便的实现SSL，具体见作者其他文章。

3.1 安装组件"证书服务"

要实现SSL，首先必须有安全认证中心。安装Windows 2000 Advanced Server的机器可以成为安全认证中心。如果在初始安装Windows 2000 Advanced Server时没有选择"证书服务"，可以通过"控制面板"->"添加/删除程序"->"添加/删除Windows组件"进入。按提示，逐步完成安装。此过程中，只需注意要选择"独立根CA"即可，其他任意。

配置CA：从"开始"->"程序"->"管理工具"->"证书颁发机构"进入，右键点击刚安装的CA，选择"属性"->"策略模块->"配置"，选择"始终颁发证书"项。完成配置。

3.2 向自己组建的安全认证中心申请安全证书

从"管理工具"->"Internet服务管理器"->"默认Web站点"点击右键，选择"属性"，点击"目录安全性"，单击"服务器证书"，在向导中，选择"创建一个新证书"。最后生成证书申请文件certnew.txt(请注意保存)。

新增一个站点（用来发布证书），设端口值为6666（1024以上可任意选取），主目录为\WINNT\system32\certsrv。

在浏览器中输入"http://localhost:6666"，根据提示，逐步选择"申请证书"->"高级申请"->"使用Base64编码的PKCS#10或PKCS#7文件更新证书申请"，在所出现的两个对话框的上一个输入文件certnew.txt中的所有内容（建议采用剪切，粘贴的方法），选择"下载证书"，完成申请安全证书。

3.3 SSL服务器的配置

如第一步，进入"证书颁发机构"，在"待批准的申请"中批准第二步申请的证书（在以后的应用中，也用类似方法批准其他客户的申请）。

安装第二步下载的证书：在"Internet服务管理器"中，选择"默认Web站点"，点击右键，选择"属性"，连续单击"目录安全性"->"服务器证书"->"处理挂起的请求并安装新证书"，然后输入文件"certnew.cer"所在的目录。退出后，再次进入"目录安全性"项目，"安全通信"栏中的"编辑"由灰色变成了黑色，点击"编辑"，选择"申请安全通道SSL"和"接受客户证书"。至此，完成SSL服务器的配置。在任意客户端可以使用SSL方式连接该服务器。

3.4 说明

在客户端，必须使用https来代替http来访问使用SSL后的服务器。使用SSL后，由于要进行复杂的交互认证过程和加密解密过程，网络传输速度大大降低。据统计，平均速度只有不用SSL时的十分之一，相对于其保密价值，这点牺牲是值得的。另外一个解决办法是，只对一些关键信息采用SSL传输，如：用户名、口令、银行卡号等，而其他的信息用普通传输，只需要把这里的对整个站点的配置改为对某个目录或文件即可。

参考文献

1 娄定俊，算法分析与设计(讲义)[M]，中山大学计算机科学系，1998。

2 Tanenbaum A S. Computer Networks .Third Edition Prentice Hall [M] 1996 。

3 高传善等，数据通信与计算机网络 [M]，高等教育出版社，2001。