Journal of Wuhan Polytechnic

采用协议重定向实现基于 HTTPS 的数据安全传输

杜　江，张丽英

（南通纺织职业技术学院，江苏　南通　226007）

摘　要： 随着 WEB 应用的拓展，WEB 服务的数据安全性问题日益突出。文中分析了 WEB 服务数据的传输通道—HTTP 协议在安全性方面的缺陷，介绍了采用协议重定向方法实现基于 HTTPS 的数据安全传输。

关键词： 数据安全；HTTP；HTTPS；SSL 协议

中图分类号： TP393　　**文献标识码：** A　　**文章编号：** 1671-931X（2012）01-0080-03

一、引言

WEB 服务是互联网上最重要、最广泛的应用之一。HTTP 协议作为 WEB 服务数据的传输通道，成为互联网上最常见、最重要的应用层协议之一。随着 WEB 应用的拓展，WEB 服务的数据安全性问题日益突出。而 HTTP 设计的初始是基于相互信任，数据在网络上的传输是采用明文，不做任何加密处理；另外，HTTP 协议在传输客户端请示和服务端响应时，唯一的数据完整性检验就是在报文头部包含了本次传输数据的长度，而对内容是否被篡改不作确认[1]，因此数据传输的安全性得不到保障。针对 HTTP 协议的安全缺陷，可通过采用 HTTPS 协议来加强安全性。

二、HTTPS 协议

HTTPS 是安全超文本传输协议，它是由 Netscape 开发并内置于其浏览器中，用于对数据进行压缩和解压操作，并返回网络上传送回的结果。实际上，HTTPS 是 SSL over HTTP，就是经过 SSL 加密后的 HTTP[2]，HTTPS 通过在 TCP 层与 HTTP 间增加一个 SSL（Secure Socket Later，安全套接层协议）来加强安全性，该协议通过 SSL 在发送方把原始数据进行加密，在接收方解密，因此，所传送的数据不容易被网络黑客截获和破解[3]。SSL 使用 40 位关键字作为 RC4 流加密算法，这对于商业信息的加密是合适的，同时，HTTPS 和 SSL 支持使用 X.509 数字认证，如果需要的话用户可以确认发送者是谁。

目前，HTTPS 在企业中的应用主要是在两个方面：SSL VPN 和 WEB 服务器。企业使用 SSL VPN 提供接入服务，使员工可以在任何地方的外部网络安全的连接到企业内部，登录企业内部的 OA 系统，处理等业务；在 WEB 服务器上使用的 HTTPS，主要是用来保护传输中的数据不被截获，可应用在内部的 OA 系统中传输需要保密的财务、人力、邮件等敏感资料，在对外提供的服务中，可保护用户的隐私不被

收稿日期：2011-11-08

作者简介：杜江（1972-），男，山西大同人，硕士，南通纺织职业技术学院信息系讲师，研究方向：计算机软件技术和多媒体应用；张丽英（1974-），女，硕士，天津武清人，南通纺织职业技术学院信息系副教授，研究方向：计算机辅助教学和多媒体应用。

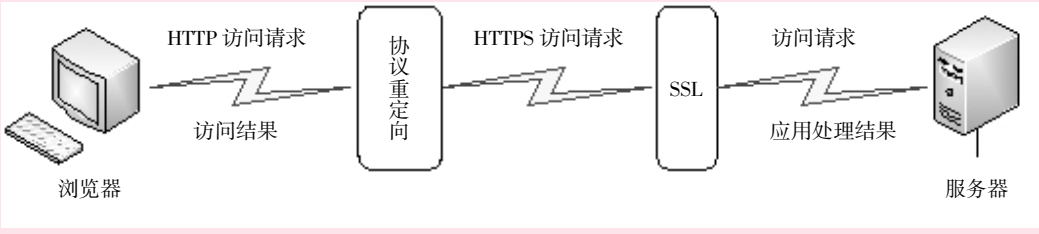

图 1 基于 HTTPS 的安全传输设计原理图

第三方泄露[4]。

HTTPS 协议的简单工作原理是：使用非对称加密的方式加密一个密钥，然后双方使用这个密钥对传输的明文数据进行对称加密。常用的非对称加密算法是 RSA，对称加密算法是 DES、AES 等，完整性检验算法是 MDS。

三、基于 HTTPS 的安全传输设计

当用户通过浏览器和远端网络服务器建立安全链接时，需要在传输时应用 HTTPS 安全传输[5]。HTTPS 的会话连接建立的过程：

1. 客户端发起连接，向服务器发送 request 报文，主要内容包括自己支持的各种算法列表，比如非对称加密支持哪些加密算法，对称加密支持哪些加密算法。

2. 服务器收到消息之后，和自己支持的加密算法对比，找出双方都支持的算法，然后服务器把自己的证书（常见的是 X.509 证书）发送给客户端，包含被选中的加密算法，X.509 证书等内容，而证书中包含服务器的公钥等内容。

3. 客户端接受到了证书之后获取服务器的公钥，随即生成一个字符串，使用服务器的公钥加密，发送给服务端。服务端用自己的私钥解开这个加密串，得到明文。然后服务器和客户端之间就使用这个串作为密钥，来做对称加密。

要实现 HTTPS 安全传输，其核心是 SSL。实现的设计原理是：首先创建一个类，该类方法可以实现自动引导 Web 客户的访问请求使用 HTTPS 协议，每个要求使用 SSL 进行传输的 Servlets 或 JSPs 在程序开始时调用它进行协议重定向，再使用 SSL 通过交换共享密钥来加密和解密数据，最后才进行数据应用处理。设计原理图如图 1 所示。

四、基于 HTTPS 的安全传输实现

根据设计原理，采用协议重定向实现基于 HTTPS 的安全传输设计的基本步骤为：

1. 获取访问的请求所使用的协议。

2. 如果请求协议符合被访问的 Servlet 所要求的协议，就说明已经使用 HTTPS 协议了，不需做任何处理。

3. 如果不符合，使用 Servlet 所要求的 HTTPS 协议重定向到相同的 URL。

4. 使用 SSL 通过交换共享密钥在发送方将原始数据进行加密，在接收方进行解密。

采用协议重定向实现数据 HTTPS 安全传输的流程图如图 2 所示。

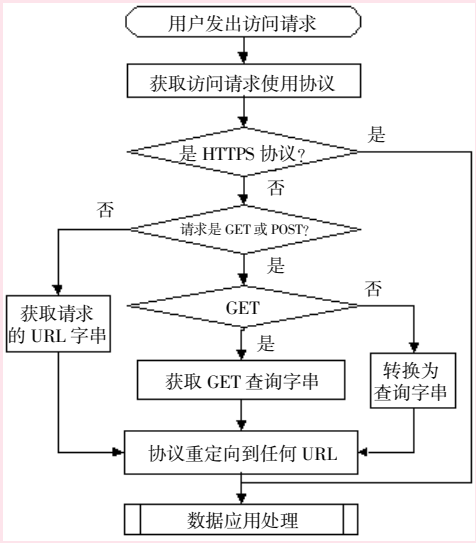

图 2 基于 HTTPS 的安全传输流程图

具体实现时，使用 Java Servlet API 中的两个方法来获取请求使用的协议：ServletRequest 接口中的 getScheme()方法，它用于获取访问请求使用的传输协议；使用 HTTPUtils 类中的 getRequestUrl()来获取访问请求的 URL，需要注意的是该方法在 Servlet 2.3 中已被移到 HTTPServletRequest 接口；使用 request.getQueryString()来获取 GET 的查询字串，对于 Post 的 Request 参数，可以把它们转换成查询串再进行处理；协议重定向可以使用 HTTPS ervletReponse 接口里的 sendRedirect()方法，它能使用任何协议重定向到任何 URL。

另外，在 Web 应用中实现还必须考虑如下几个问题：

1. 在 Web 应用中常常会用到 GET 或 Post 方法，访问请求的 URL 中就会带上一些查询字串，这

些字串是使用 getRequesUrl()时获取不到的，而且在重定向之后会丢失，所以必须在重定向之前将它们加入到新的 URL 里。我们可以使用 request.getQueryString()来获取 GET 的查询字串，对于 Post 的 Request 参数，可以把它们转换成查询串再进行处理。

2. 某些 Web 应用请求中会使用对象作为其属性，必须在重定向之前将这些属性保存在该 Session 中，以便重定向后使用。

3. 大多数浏览器会把对同一个主机的不同端口的访问当作对不同的主机进行访问，分用不同的 Session，为了使重定向后保留使用原来的 Session，必须对应用服务器的 Cookie 域名进行相应的设置。

下面是实现的部分代码：

```
response. setCharacterEncoding( "utf-8");
String key =fromId +String.valueOf (Calendar.getInstance().getTimeInMillis());
infoForVideoRequest.put(key, returnXmlValue);
//定向到服务器任何名为 page_name 的 URL 页面
responsesendRedirect("https"+requestgetQueryString().substring(4)+"/page_name 十 key);
```

五、总结

可以预见，随着硬件和 WEB 理念的发展，HTTPS 协议将会在 WEB 应用中发挥越来越大的作用。通过采用重定向协议，实现了安全的 HTTPS 连接，对所发文字、音视频等数据进行了加密，实现了信息的安全传输。

参考文献：

[1] 吴维元，肖柳林，李荣辉.Web 服务数据传输通道的安全性分析[J].网络安全技术与应用，2008，(2):85.

[2] Scott Oaks. Java 安全(第二版)[M].北京：中国电力出版社，2002.

[3] 陆荣杰，刘知贵，郑晓红.基于 HTTPS 隧道技术的统一认证平台与实现[J]. 计算机应用研究，2006，(12):168

[4] 魏兴国.HTTP 和 HTTPS 协议安全性分析[J].程序员，2007，(7):55.

[5] Thawatchai Chomsiri. HTTPS HackingProtection [J]. IEEEComputer Society，2007:590-594.

[责任编辑：刘　骋]

Realizing Data Transmission Security with Protocol Redirect Based on HTTPS

DU Jiang　ZHANG Li-ying
(Nantong Textile Vocational Technology College, Nantong 226007, China)

Abstract: With the extension of WEB application, the data security of WEB service is becoming an outstanding problem. In this paper, the security flaws of HTTP protocol- the WEB service data transmission channel are analyzed, and the method of protocol redirect based on HTTPS is introduced to enhance the security of data transmission.

Key words: data security; HTTP; HTTPS; SSL Protocol

（上接第 64 页）

Package Design Innovation- Access to Development of Tea Brand

ZHU Feng
(Department of Business Administration, Gungdong Baiyun University, Guangzhou510450, China)

Abstract: The paper discusses the approach to promoting the brand of tea products. It has been found that the package of tea products is out of date in design, which cuts down the consumer's credence and hinders the value communication, inducing overpackaging. It is advised that the design of the tea packaging should break with traditions and the tea should be labeled completely. Tea package innovation can not only promote tea brands building, but also boost the restructure of tea industry.

Key words: tea; brand; package