

Web-Web 间网络安全传输的研究

王华香¹, 鲁向前²

(1. 广东工业大学 信息工程学院, 广东 广州 510006; 2. 韶关市商业学校, 广东 韶关 512000)

摘要: 讨论了网络传输中对安全的攻击种类和安全服务要求, 依据 SSL(secure sockets Layer) 的设计思想, 着重对 Web-Web 之间的网络安全传输进行研究, 并提出可行的加密解密和安全传输的算法实现.

关键词: Web-Web; SSL; 安全传输

中图分类号: TP315 文献标识码: A 文章编号: 1007-7162(2006)02-0103-06

在网络安全传输中, 一般都是指 B-Web(浏览器 Web 服务器) 之间传输. B-Web 之间的安全传输是在浏览器与 Web 服务器之间建立一个安全通道, 利用 SSL(secure sockets Layer) 在传输层建立一个安全连接通道来实现浏览器和 IIS Web 服务器之间的标准安全传输. 然而对于 Web-Web(Web 服务器-Web 服务器) 之间的 SSL 实现却还没有一定的标准. 本文基于 SSL 的设计思想, 对 Web-Web 之间实现安全传输进行研究.

1 网络传输中对安全的攻击种类和安全服务要求

对网络安全的设计是基于对网络安全攻击的种类分析而采用不同的安全防范手段. 网络传输中对安全的攻击是指在通信双方的正常通道上出现了不相干的第 3 方, 对通信的数据进行中断、伪造(重放)、篡改、截获(解密)等破坏性的动作, 使正常的通信变得不可用或不可靠. 如图 1 所示. 网络传输安全服务包括保证数据信息的机密性、完整性、发送方和接收方的不可抵赖性以及可用性.

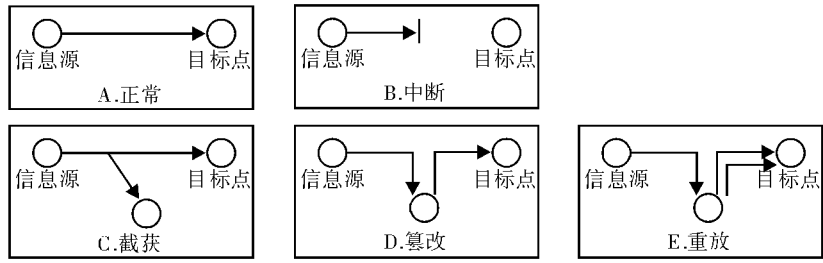


图 1 攻击的种类

2 SSL 简介

SSL 是由 Netscape 公司开发的一套 Internet 数据安全协议, 当前版本为 3.0. 它已被广泛地用

收稿日期: 2005-12-28
作者简介: 王华香(1967), 女, 实验师, 主要研究方向为信息管理系统.

于 Web 浏览器与服务器之间的身份认证和加密数据传输.

SSL 协议位于 TCP/IP 协议与各种应用层协议之间, 为数据通讯提供安全支持, SSL 协议可分为两层:

- 1) 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.
- 2) 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, 通讯双方进行身份认证、协商加密算法、交换加密密钥等^[1].

3 Web-Web 的加密解密设计

一般的信息安全传输系统, 主要由两部分组成: 一部分进行信息加密和数字签名, 称为发信过程; 另一部分对信息验证签名和数据解密, 称为收信过程^[2], 发信和收信过程中都必须保证信息的机密性、完整性和不可抵赖性. 同样的, 本文所讨论的 Web-Web 之间加密解密算法主要针对传输中的机密性、完整性、不可抵赖性而设计, 加密流程如图 2 所示.

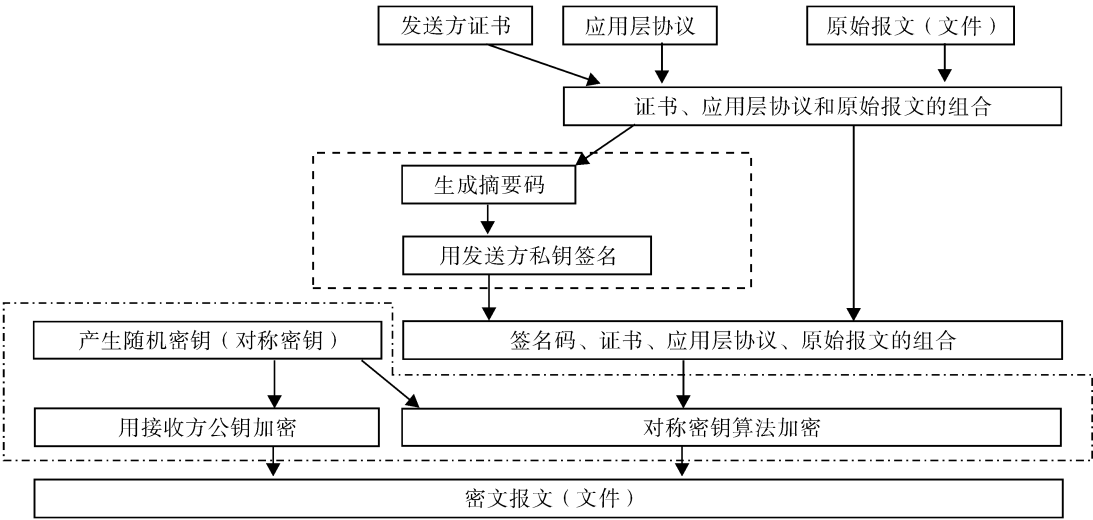


图 2 加密流程

加密流程如图 3(a) 所示. 对于加密的实现, 运用图 3(a) 所示的方法. 解密流程如图 3(b) 所示. 解密的实现按照图 3(b) 所示的方法进行设计^[3].

用算法表示加密过程如下:

```
bool Sf_To_Df( void & DestPackage, char * ScertFile, char * SDatabase, char * STable, char * DHost, char
* DDatabase, char * DTable, char * OperateType )
{
    生成应用层协议;
    组合证书、应用层协议和源报文= >>NewPackage1;
    EVP_Sign( NewPackage1, Private_Key )= >>NewPackage2;
    EVP_Seal( NewPackage2, Public_Cert )= >>DestPackage;
}
```

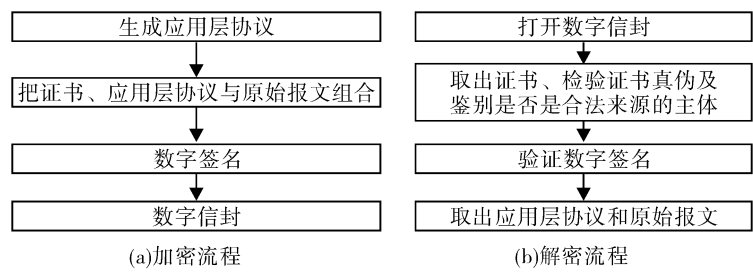


图 3 加密解密的实现

进行传输前, 先为需传输的报文(文件)产生应用层协议, 应用层协议应根据应用层具体情况可扩展, 因此应用层协议设计成包含若干协议域的形式, 每一个协议域包括两部分: 长度和内容, 在所有协议域前面设计一个总协议域长度值^[4]. 应用层协议的组成图 4 所示.

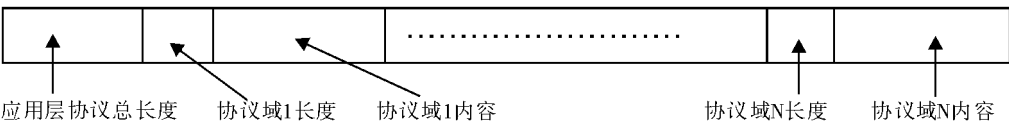


图 4 应用层协议描述

在实际应用中, 至少应包括如下协议域: 报文源主机、报文源数据库、报文源数据表、报文目标主机、报文目标数据库、报文目标数据表、报文到达目标点后的操作类型等.

4 Web-Web 安全传输试验

4.1 商务逻辑实现的方法

商务逻辑是指在系统中机密性极高或者流程最重要的那部份逻辑, 通常会涉及到软件使用单位的核心商业秘密和软件流程等的秘密. 实现商务逻辑有两种方法.

第 1 种方法是直接把商务逻辑程序写在 ASP 程序里. 这种方法实现商务逻辑是非常不安全的, 原因是 ASP 程序是解释性代码, 在执行前不需要编译, 因此对于 Web 的管理人员或者主机的攻击者都非常容易接触到源代码, 也就是接触到软件使用单位的核心机密, 然后可以非常方便地进行修改, 可以把正逻辑改成负逻辑, 就会造成软件使用单位的核心机密的泄露. 比如在考试系统中, 对于试题的机密性极高, 如果 Web 管理人员或主机攻击方把加密逻辑改成不加密就发送出去, 那么所有收到试题的用户都是收到明文, 那么整个考试就失去了公平性.

第 2 种方法是把商务逻辑程序写成 DLL, 再由 ASP 程序调用. 这种方法是安全的, 因为 DLL 是一种编译好的共享二进制程序. 这样即使 Web 管理人员或者主机攻击者获得了 DLL, 但他也不能读懂其中的逻辑, 更不可能修改其中的逻辑了. 比如对于上面的例子, 如果把考试系统试题安全传输的逻辑写成 DLL, 那么就可以从根源上保证传输之前的安全.

4.2 DLL 实现方法

第 1 种方法是使用非 COM(Component Object Model) 技术实现 DLL. 所谓非 COM 技术是指 COM 技术出现之前的编写 DLL 程序的方法和技术. 非 COM 技术有两个缺点(对 C++ 来讲): 第 1 个缺点是 C++ 类是用于源代码重用而设计的. 因此 C++ 类只能在 C++ 程序里使用, 而不能在其它编程环境中使用其源代码, 如果要使用, 必须要修改源代码. 第 2 个缺点是尽管 C++ 类可以用源代码形式发布, 但是也可以用 Windows Dll 形式发布, 但在 COM 之前, 类的成员函数

只能以简单的 C 类型函数形式发布, 因此即使别人共享你的 DLL, 但也不能使用面向对象的程序设计的优越性了^[5].

第 2 种方法是使用 COM 技术. COM 又称组件对象模型. 它的主要优点是实现了对象间的通信标准, 还可使编程人员在实现二进制代码的共享的同时保持面向对象的程序设计方法.

4.3 服务器类型的选择

服务器程序必须能够并发处理多个客户机的服务请求, 编写服务器程序有 3 种模式: 循环处理技术、消息驱动技术、多线程技术.

循环处理方式的服务器程序提供的服务能力是有限的, 因为这种方式编写的服务器程序只有一个线程, 如果服务器正在为一个客户机提供服务, 而另一个客户机同时向它提出服务请求则不会得到响应. 假若前面的客户机在享受服务的同时有人机交互, 那么服务器程序也必须等待, 直到该服务完成, 因此这种方式的服务器程序通常只用于人机交互少、服务时间短的情况.

消息驱动方式的服务器程序是使用 Windows 提供的消息驱动技术, 因此它可以非常方便地实现并发处理. 然而服务器程序无法预知消息的发生时刻, 所以很难确切地知道代码的实际执行顺序, 也就保证不了程序的逻辑顺序.

Windows 的多任务调度技术使得服务器可以给每个客户机创建一个线程, 独立地处理请求和应答, 一个处理线程的阻塞不会妨碍其它线程的服务正常进行, 因此是开发 Windows 服务器程序的理想方法.

4.3.1 NT 服务程序的结构

基于 NT 技术的服务器程序是在后台悄悄运行的, 服务器程序应该具备一些基本的功能, 比如: 启动服务、暂停服务、停止服务等.

Windows 有一个重要的操作系统程序——服务控制管理程序, 系统中由它管理所有基于 NT 技术的服务器程序, 比如我们常见的 IIS, FTP 等典型的服务程序都是由服务控制管理程序进行控制.

服务控制管理程序提供了统一和安全的接口, 使得程序员只要遵照接口标准就可以方便地编写出自己的服务器程序.

服务器程序通常写成控制台类型的应用程序, 一个完全遵守服务控制管理程序标准接口的服务程序必须包含下面 3 个函数:

- 1) 服务程序主函数(main): 由它调用系统函数 StartServiceCtrlDispatcher, 由它把服务程序主线程连接到服务控制管理程序;
- 2) 服务入口点函数(ServiceMain): 执行服务初始化任务, 同时执行多个服务的进程有多个服务入口点函数;
- 3) 控制处理程序函数(Handler): 在收到服务控制管理函数的控制命令后执行, 由它处理暂停、停止等命令的具体细节.

另外服务程序还必须能实现安装、删除等任务, 完成在注册表中的系统注册和删除. 它们是在命令行带指定参数时执行.

可以用图 5 来表示 NT 服务程序的框架结构, 图中箭头表示调用关系.

4.3.2 协议解释线程函数的实现

在图 5 中的服务功能主函数里, 主要完成两个功能: 一是在主线程上创建一个监听套接字 (有 21 号端口); 二是在有连接请求时先初始化信号灯, 然后创建新线程.

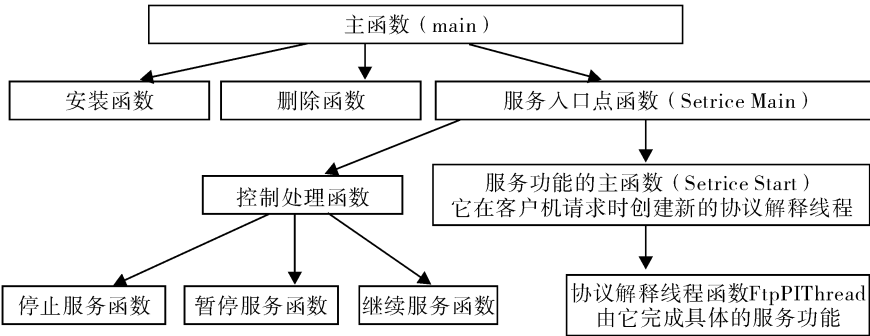


图 5 NT 服务程序框架

图 5 中的协议解释线程函数是整个服务器功能的具体体现,即服务器编程的大部份代码都在这里实现.实现 Web-Web 间的安全传输的算法如下,要注意这里的协议是遵从标准的 FTP 协议,并增加了安全功能和数据库的访问功能:

```
unsigned _stdcall FtpPThread( void * pArg)
{
while( true)
{ 获得命令动词; 第一个命令动词必须是 USER;
判断是否是合法用户,这里的用户名是指下级 Web 的浏览器的用户名
}
while( true)
{ 获得命令动词; 第二个命令动词必须是 PASS;
判断密码是否正确
}
while( true)
{ 获得命令动词;
如果命令动词是 PORT: 端口处理,向客户端发起反向数据连接请求;
如果命令动词是 TYPE: 设定传输文件的类型(二进制或文本);
如果命令动词是 STOR:
{
接收数据;
计算消息摘要码;
检索消息摘要码,如果检索到,则丢弃, break;
存储消息摘要码;
//为了安全,接收到的数据并不作为文件保存,而是直接在内存处理
解密;//具体算法请参见图 3(b)
写入数据库服务器的相应数据库内;
}
如果命令动词是 RETR:
```

```
从数据库服务器获取相应数据;  
//为了安全, 获取的数据不作为文件保存, 而是直接在内存处理  
加密;//具体算法请参见图 3(a)  
把数据发送到请求方;  
}  
}  
}
```

5 结语

根据以上的分析研究, 能较好地解决 Web-Web 之间的网络安全传输问题, 我们将此研究应用在我们的开发项目: 基于 Internet 的考试系统中的敏感数据(试卷、答卷和成绩)的网络传输, 效果良好. 网络安全传输是一个不断发展的研究课题, SSL 是一个内容非常丰富的软件包, 加密解密算法和理论都在不断的发展, 网络工程的应用和需求也在跟随着发展, 分布式协作式安全网络有着广泛的研究前景, Web-Web 间的安全传输还有很大的研究空间.

参考文献:

- [1] 吴凯, 陈晓苏, 肖道举. 网络传输层安全协议 SSL 的安全性研究[J]. 计算机系统应用. 2003, (1): 50-52.
- [2] 杨旭东. 基于 PKI 的信息传输安全系统[J]. 唐山学院学报. 2003, 16(1): 10-11.
- [3] 鲁向前. 基于 Internet 的网络考试系统网络传输安全的研究和实现[D]. 华南理工大学硕士学位论文. 2004.
- [4] 杨明, 胥光辉, 齐望东, 等译. 密码编码学与网络安全原理与实践(第二版)[M]. 北京: 电子工业出版社. 2001: 61-62.
- [5] 李博轩. Visual C++ 6.0 网络及 Internet 开发指南[M]. 北京: 清华大学出版社. 2000: 84-85.

Research on Safe Network Transmission between Web and Web

WANG Hua-xiang¹, LU Xiang-qian²

(1. Faculty of Information Engineering, Guangdong University of Technology, Guangzhou 510006 China,

2. Shaoguan Business School, Shaoguan 512000, china)

Abstract: The paper discusses attack categories and demand of security service, Based on the thinking of SSL, the security of network transmission between Web and Web is deeply studied and the method of workable encryption, decryption and safe transmission is expounded.

Key words: Web-Web; SSL; safe transmission