一个面向开放环境的安全传输平台

樊隽 龚俭

（东南大学 计算机系，210096 南京）

【摘要】本文介绍了一个面向开放环境的安全传输平台的设计与实现，保证了在开放环境下通信双方的安全连接和数据传输的安全性。主要工作是利用 PGP 中已有的数据加密、数字签名和密钥管理技术等，实现通信双方的安全通信，包括安全连接的建立、撤销，数据的安全传输和密钥管理。

【关键词】身份认证；数字签名；密钥管理；PGP

中图分类号：TP393

A circumstance oriented secure tranport system

Fan Jun, Gong Jian

(Southeast University, Computer Science Dept., 210096 Nanjing, P.R.China)

【Abstract】This paper discussed the design and implementation of a circumstance oriented secure tranport system in detail, ensure the security of the connection between the client and server and the data transport. The main task is to implement the secure communications between the client and server, including the establish of secure connection, the repeal of the connection, the data's secure transfer and the key management, based on the data encrypting、digital signature and key management of PGP.

【Key words】authentication;digital signature;key management;PGP

1.引言

Internet 追求简洁和开放的思想给它带来了许多的安全隐患，这对其上涉及敏感数据的应用的开发和普及产生了很大影响。人们不能保证正在和你通信的人就是你认为的那个人，也不能保证你传输的数据没有被窃听、篡改、破坏，因此，实现一个安全的传输平台的要求就很迫切，它可以提供通信环境下的安全支撑。

通过建立一个安全传输平台，可以解决用户之间的加密、鉴别和数据完整性的维护的问题，可以防止非法用户利用网络系统的安全缺陷进行数据的窃取、冒充和破坏。运用一个这样的安全传输平[1]台，

---

[1] 作者简介：樊隽，本科生，主要研究方向为网络安全。

龚俭，工学博士，东南大学计算机系教授、博导，主要研究方向包括网络管理、网络安全、网络体系结构、开放分布式处理等。

定稿日期：2000-06-26

你就不用担心和你通信的是冒充者，也不用担心你的数据被泄漏。在这种情况下，华东（北）地区网络中心开发了此安全传输平台。它实现了数据加密、数字签名等功能，保证通信双方的安全连接，避免第三者冒充和桥间攻击，在数据传输的过程中，数据是以加密的形式传输的，保证了数据的安全。同时，数字签名技术保证了用户的身份，提高了可靠性，还用于用户行为的无否认。定义的报文格式和传输机制还保证了数据的完整性。总体来说，安全传输平台可以应用于多项安全应用系统，它提供了底层的安全支撑环境，目前，我们把此安全传输平台应用于国家 863-317 课题和远程教育系统。

在安全传输平台的实现中，我们要用到 PGP 中的相关技术。PGP 的全称是 Pretty Good Privacy，它是 Internet 上一个著名的共享加密软件，与具体的应用无关，可独立提供数据加密、数字签名、密钥管理等功能，适用于电子邮件内容的加密，和文件内容的加密；也可作为安全工具嵌入应用系统之中。

2. 安全传输平台体系结构

本安全传输平台建立在 IP 层以上，应用层下，基于 TCP 进行面向连接的传输，它为其他应用程序提供了一个安全接口，包括安全连接的建立 sec_connect，连接的释放 sec_close，安全传输数据的读取 sec_read 和安全传输数据的发送 sec_write。同时，它还提供了几个底层的函数接口，包括加密函数 encrypt、解密函数 decrypt 和签名函数 sign。

系统总体结构框图如图 1 所示，主要分为三个大模块：连接管理、数据传输和密钥管理。其中，密钥管理模块交叉在其他两个模块中，因为连接管理中通信双方的身份认证，数据传输中数据的加密、签名都涉及到公钥的分发、私钥的保存等密钥管理中的内容。从实现上说，每个部分又涉及到数据加密、密文解密、数字签名。下面分别对各个部分详细讨论。

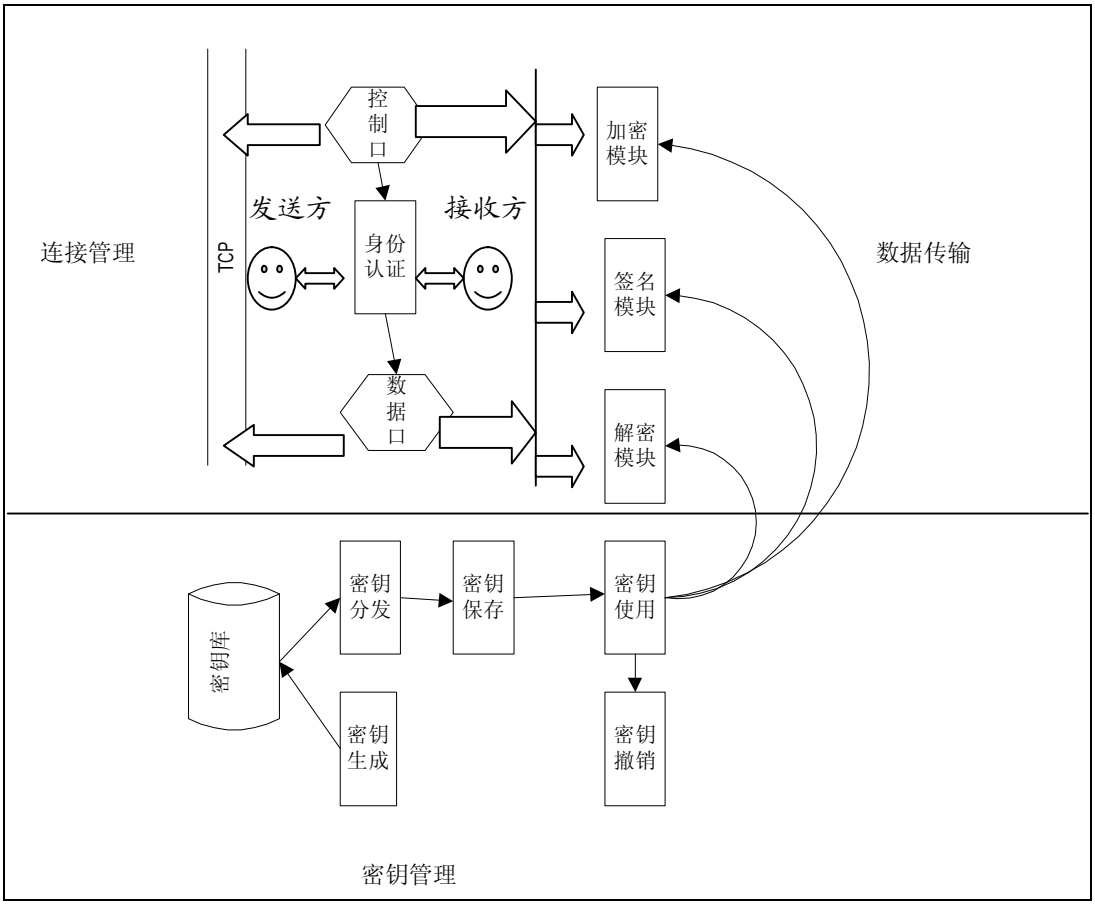

图 1 系统总体结构框图

连接管理包括建立连接和释放连接，又分为常规连接和安全连接，安全连接要对通信双方进行双向鉴别和身份认证，且数据全部采用公开密钥体制进行加密，以确保双方没有被第三者冒充。因此，我们采用双向鉴别的公开密钥改进模型作为建立连接的安全模型。常规连接没有双向鉴别和身份认证，仅仅建立普通的 socket 连接，我们在这里主要讨论安全连接。

当通信双方完成了通信后，就可以关闭连接，释放套接字。但是由于 TCP 允许双向通信，因此，关闭一个连接需要在客户机和服务器之间进行协商。当客户机结束发送请求时，可以使用部分关闭来指明没有数据发送了，但并不释放套接字；服务器在发送完最后一个响应后就可以关闭这个连接，释放套接字。

在通信双方建立起连接后，就可以进行数据传输了。同样，为了防止第三方采用攻击方式截取数据、篡改数据或进行桥接攻击，就需要在数据传输时，把数据加密成密文方式；为了防止通信双方的行为否认或第三方的冒充，就需要进行数字签名和加密。因此数据传输也采用两种方式：普通传输方式和安全传输模式。在安全传输模式下，我们必须保证传输数据的安全性。因此，在发送方，我们需要公钥加密、数字签名，在接收方，我们需要私钥解密、数字签名核实，即数据传输要包含加密、解密、签名、加密签名四个功能。在实现中，加密、解密、签名模块我们采用 PGP 方式，即根据 PGPsdk 提供的静态函数库，实现这些具体的函数功能。

在安全传输平台的设计中，密钥管理是很重要的一环。在建立连接时，通信双方要进行身份认证和双向鉴别，这需要用到对方的公钥和自己的私钥。在数据传输时，采用公开密钥体制进行加密，也涉及到对方的公钥和自己的私钥；数字签名同样需要用到私钥。同时，这些还涉及到密钥的保存、分发、信任关系等。而密钥的泄漏将直接导致明文内容的泄漏，因此，密钥管理模块格外重要。密钥管理模块包括密钥的生成、撤销、验证、签名、使用、保存和传递等。

如上所述，加密采用的是 PGP 中的加密方式，即通信双方使用不同密钥的公开密钥体制(Deffie_Hellman 算法)，同时，还要涉及到对称密钥体制的 IDEA 加密算法。本平台中的数字签名采用的是基于信息摘录（MD5）的数字签名技术。

3. 安全传输平台的功能实现

3.1 连接管理

Ø 建立连接

模型的选择

在建立连接时，我们选择双向鉴别的公开密钥改进模型。如图2所示：

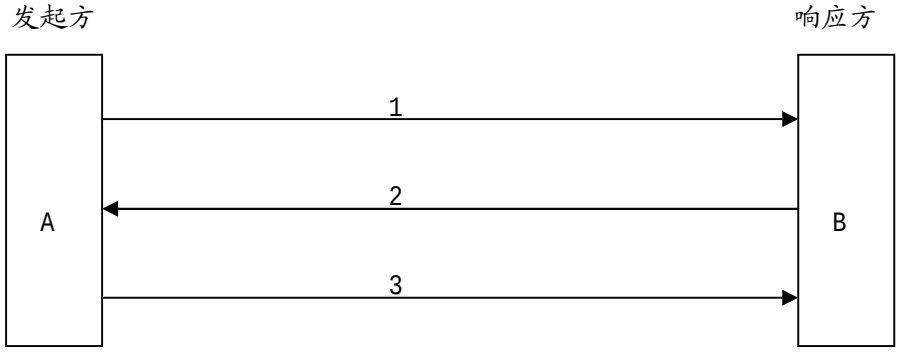

图 2 安全模型图

发起方 A 和响应方 B 之间进行三次握手，它们之间的交互采用公开密钥体制，这样可以防

止桥接攻击，同时，A、B 双方采用不同的明文值进行加密，使每一方的明文带有一定的特征。

三次握手过程为：

1.发起方 A 产生随机数 R1，R2，用 A 的私钥加密 R1 成 Ka(R1)，用 B 的公钥加 R2 成 Kb(R2)，发送 Ka(R1)、Kb(R2)；

2.响应方 B 接收到 Ka(R1)、Kb(R2)后，用 A 的公钥解密 Ka(R1)成 R1，用自己的私钥解密 Kb(R2)’成 R2，产生随机数 R3，用 A 的公钥加密(R1⊕R2)成 Ka(R1⊕R2)，再用自己的私钥加密 R3 成 Kb(R3)，发送 Ka(R1⊕R2)和 Kb(R3)。

3.A用私钥解密Ka(R1⊕R2),再用B的公钥解密Kb(R3)成R3，检查Ka(R1⊕R2)解密后的数值Ka(R1⊕R2) 是否为R1⊕R2，正确就用B的公钥加密R3成Kb(R3)，发送Kb(R3)，否则说明B方出错或不是A真正算与之通信的B，返回错误号后，断开连接。B解密Kb(R3)，检查解密后的数值是否为R3，正确，说明A的身份正确，连接建立成功，否则，断链，释放套接字。

至此，A 、B双方的身份认证完成。在此过程中，A、B双方都要用对方的公钥进行加密，从上面这个安全模型中，我们可以看出它采用了公开密钥体制，可以防止桥接攻击。在A、B双方身份认证完成后，连接就建立好了。我们把这个建立好的连接作为数据传输的控制口，用来监测数据的传输，发送控制命令等，然后我们在选用另一个端口建立一个用于传输数据的数据口。

我们采用的这种安全模型和经典的双向鉴别的公开密钥模型象比较，安全强度更加高。经典的模型在发起连接时，只传送一个随机数R1，同时传递了自己的id号来表明自己的身份，而我们采用的模型发送了里两个随机数R1和R2,一个用来加密，一个用于签名，也就是说，它没有传送自己的id，只是通过数字签名来表明自己的身份；同时，它对随机数的选择没有奇数、偶数的限制。由于不涉及到双方的id号，它的安全强度更高些，但由于此安全模型涉及的随机数加、解密次数多，运算量大，因此，速度较慢。

状态转换图

建立连接的过程中，发起方、响应方的状态转换情况分别如图 3、图 4 所示。

在任何时候，都存在断链的可能性，所以设一超时计数器，当超时,返回错误。

图中显示的是，在不超时的情况下的工作状态。

发起方：

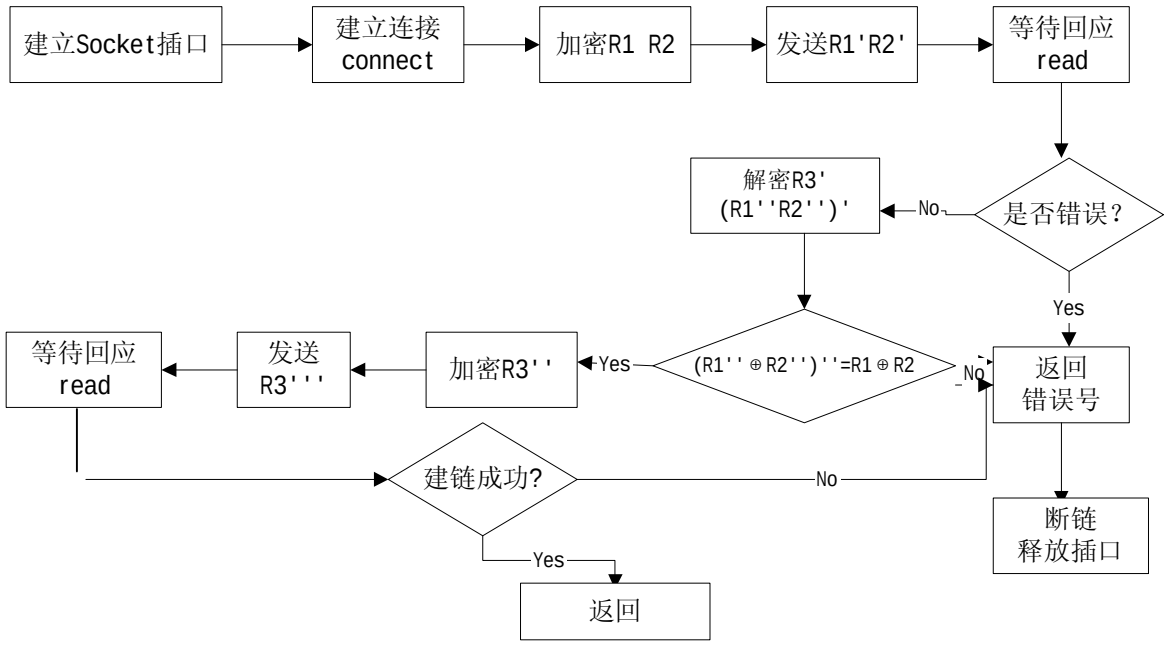

图 3　发起方状态转换图

接收方:

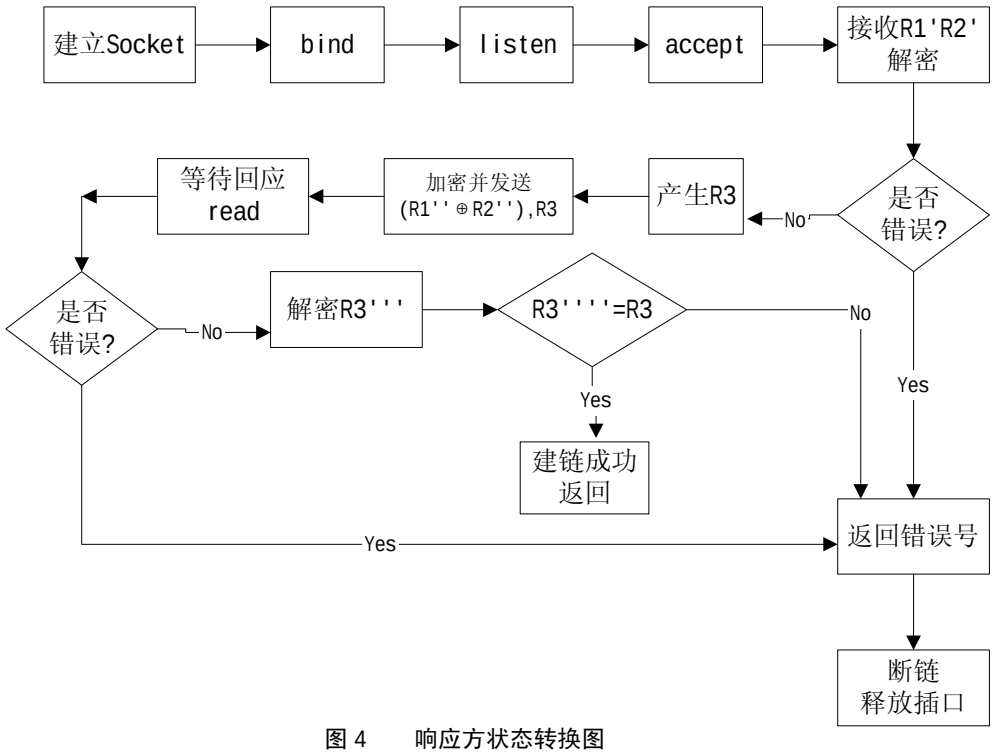

图 4　响应方状态转换图

Ø　释放连接

当通信的一方 A 打算结束通信，由控制口发送一个请求断链的报文（报文格式如前所述），另一方 B 接受到拆链请求后，检查数据口的数据传输是否完成，部分关闭数据口连接，发送拆链响应或拒绝，关闭控制口，完成拆链。

3.2 数据传输

数据传输是基于TCP的传输，包含加密、签名、加密签名、解密等功能模块，其中，加密、数字签名等均采用PGP的工作模式。用户的数据传输在数据口进行,但同时控制口依旧工作,负责监控数据的传输。数据口是由控制口产生、关闭的,报文格式为

id	length
content	

对数据的解释，由数据加密、解密层决定。

我们在安全传输平台的设计和实现中,信息的加密、解密、数字签名和密钥管理采用的都是 PGP 模式。通信双方首先调用建立连接模块，进行身份认证，完成安全建链；发送方对发送数据调用加密签名模块进行加密、签名，然后发送数据；而对方在接收到数据后，调用解密模块，验证发送方的签名，并用自己的私钥解密数据。从而，完成了一次数据传输。在双方进行数据传输的过程中，始终在数据口进行，控制口进行监控，由于是基于 TCP 传输的，保证了丢失重传。

4. 安全传输平台的改进

首先，目前本安全传输平台可以运行在 Linux 和 Solaris 系统下，但还不能够运行在 NT 环境下，这在以后可以进行改进。这部分工作实现不是很难，只需要进行部分代码的移植。

其次，此安全传输平台的数据传输是基于 TCP 的，今后，可以完成基于 UDP 的传输方式。

最后，目前在安全传输平台的实现中，我们只提供了五个接口函数，供别的应用程序进行调用，今后还可以用 PHP 编制出此安全传输平台的界面，这部分工作在假期完成。

5. 结束语

随着 Internet 的迅速发展，网络的安全问题越来越重要，对数据的安全传输的要求也会越来越高。这篇文章和依据其设计及实现的安全传输平台就是为了解决数据安全传输的问题而做出的尝试，但仍需进一步的完善。

参考文献

1. Kay A. Robbins Steven Robbins:《实用 UNIX 编程》
2. 龚俭:《计算机网络安全概论》
3. 刘建航:《基于 CA 的公开密钥管理框架》[硕士论文]
4. Rfc 2440: 《OpenPGP Message Format》
5. Douglas E.Comer David L.Stevens 《用 TCP/IP 进行网际互连》 第三卷