基于 PKI 的安全文件传输系统的设计与实现

韦昌法， 徐向阳
（湖南大学 计算机与通信学院，湖南 长沙 410082）

摘 要：阐述了基于 PKI（公开密钥基础设施）的安全文件传输系统的设计过程与实现细节。分析了安全文件传输系统所要达到的目标，引入了 PKI 技术，利用数字证书对文件进行数字签名、加密等安全处理，并在接收端进行相应的解密、验证签名等安全处理，以保障传输的文件的机密性、完整性并验证文件的来源，从而实现文件的安全传输。

关键词：PKI； 数字证书； 加密； 解密； 数字签名； 验证签名
中图法分类号：TP309 **文献标识码**：A **文章编号**：1000-7024 (2006) 01-0114-03

Design and implementation of secure file transfer based on PKI

WEI Chang-fa， XU Xiang-yang
（College of Computer and Communication， Hunan University， Changsha 410082，China）

Abstract：The design processes and implement details of secure file transfer based on PKI（Public Key Infrastructure）were shown. The aim of the secure file transfer was analyzed， introducing PKI technology. Files were signed and enerypted using digital certificate， The signatures at the receiver were decrypted and verified to ensure the security， integrity of the files and validate their sources and to implement secure file transferring.

Key words：PKI； digital certificate； encrypt； decrypt； digital sign； verify signature

1 引 言

当前，网络文件传输是网络信息传输的主要方式之一，进行网络文件传输的方式很多，我们可以通过 Web 页、电子邮件进行传输，还可以利用 QQ、MSN 等即时通信工具以及各种点对点工具进行传输。然而，不论以上述哪种方式进行传输，数据最终都要依靠底层网络通道进行传输，在传输的过程中数据包很可能被攻击者截获，进而被解包分析甚至被篡改，所传输的信息就会泄漏。因此，当我们要传输需要保密的文件信息时，就必须在传输前后对文件进行必要的安全处理，以保障文件传输的安全。

2 PKI 简介

PKI(Public Key Infrastructure)即公开密钥基础设施，它是一种遵循既定标准的密钥管理平台，是我们保障文件传输安全的有利工具。

传统的单钥密码算法采用特定的密钥对数据进行加密，解密时所使用的密钥与加密时所使用的密钥相同，因此这种算法也称为对称密码算法。将单钥密码算法应用于网络数据加密传输会不可避免地出现安全漏洞，这是因为发送方除了要将密文发送给接收方之外，还要将密钥通过网络传输给接收方，一旦攻击者截获了密文，他只需再截获相应的密钥即可将密文解密。

区别于单钥密码算法，公钥密码算法使用一对密钥，用户产生一对密钥后，将其中的一个向外界公开，称为公钥；另一个则自己保留，称为私钥。任何获悉用户公钥的人要向用户发送信息，只需用用户的公钥对信息进行加密，将密文发送给用户便可。公钥与私钥之间的依存关系确保了在用户安全保存私钥的前提下，只有用户本人才能对密文进行解密，任何未经用户授权的人都无法对此密文进行解密。

PKI 就是利用公钥密码理论和技术建立起来的提供安全服务的基础设施，它是信息安全技术的核心，也是电子商务的关键和基础技术，它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。

通常，一个完整的 PKI 系统必须具有权威认证机构(CA)、数字证书库、密钥备份及恢复系统、证书作废系统和应用接口(API)等基本组成部分。

3 系统的设计和实现

3.1 系统目标分析

作为一个安全文件传输系统，系统必须达到以下目标：①保障数据机密性：系统必须确保只有预期的文件接收方才能读取文件信息；②保障数据完整性：文件接收方能够验证他所接收到的文件是否完整，是否在传输过程中被非法篡改过，以保证他接收到的文件与发送方发送出来的文件完全相同；③对

收稿日期：2004-12-10。
作者简介：韦昌法 (1982-)，男 (壮族)，广西巴马人，硕士生，研究方向为信息安全； 徐向阳 (1973-)，男，湖北麻城人，副教授，博士，硕士生导师，研究方向为信息安全。

数据源的身份验证:文件接收方可以验证文件是否确实是由指定的发送方发送过来的;④网络信息成功收发:系统必须确保发送方能够成功地将文件以及必要的即时消息传输给接收方。

3.2 系统设计概述

为了实现上述目标,系统将通过高强度的、安全可靠的加密技术对文件进行加密,以防止攻击者截获文件数据后能成功进行破解而导致文件信息泄漏,完善的加密技术尽可能做到使攻击者无法解读其所截获的数据包中的信息。

系统还将对文件进行数字签名以及相应的验证签名处理,以使文件接收方可以判断出文件在传输的过程中是否已被篡改以及文件是否确实是由指定的发送方发送过来的。数字签名技术还保证了文件信息的不可否认性,即如果用户确实向其他用户发送了某一文件,他将无法对此进行否认。

通过引入PKI技术,利用数字证书对文件进行数字签名、加密等安全处理后再通过网络进行传输,接收方接收到文件之后相应地对文件进行解密、验证签名等安全处理,系统将能够保障文件的机密性、完整性并验证文件的真实来源,实现文件的安全传输。

在网络数据的传输方面,系统通过 Windows Socket 套接口编程技术建立通信双方之间的连接,并自定义一个简单的通信协议,这一协议的核心是双方所发送的数据包的格式,通信双方将严格按照这一协议进行通信、传输文件、即时消息和连接控制消息。

3.3 系统模块划分

根据上述的系统目标以及系统设计概述,我们将系统划分成两大模块,即安全处理模块和网络传输模块。

其中,安全处理模块主要负责对文件进行数字签名、加密、解密和验证签名等安全处理;由于系统使用了数字证书,所以访问公钥基础设施,辅助用户申请、查询和下载数字证书,将数字证书安装到操作系统证书库中,查看和删除用户已安装的数字证书等,也是安全处理模块所要兼顾的功能。而网络传输模块则主要负责建立和管理通信双方之间的通信连接,以在两者之间传输文件和消息。系统结构如图 1 所示。

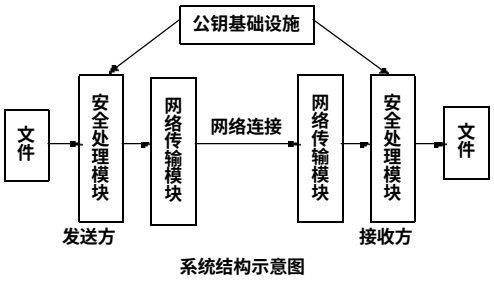

图 1 系统结构

3.4 安全处理模块的具体实现

为了保障文件传输的安全,发送方首先要对文件进行数字签名处理,接着进行加密处理,然后才将处理后的文件传输给接收方,接收方接收到文件之后要先进行解密处理,然后进行验证签名处理,验证无误后方可读取文件信息。当然,用户也可以根据实际的安全需求只对文件进行加密处理或数字签名处理,这样接收方在接收到文件后将只需相应地进行解密处理或验证签名处理。上述这些安全处理操作都是由系统的安全处理模块来完成的,下面将逐一介绍。

(1)对文件进行数字签名:根据PKI的理论,发送方将用自己的私钥对文件进行数字签名,接收方在接收到经过签名处理的文件之后将用发送方的公钥进行验证签名,根据验证签名的结果判断文件在传输的过程中是否已被篡改以及文件是否确实是由指定的发送方发送过来的。

对文件进行数字签名时,发送方要用到他自己的私钥,在用户申请数字证书时,CA会将这一私钥提供给用户或直接将它安装到用户的电脑上,这一私钥也可能包含在用户自己持有的特殊的数字证书当中,在进行签名之前用户必须在自己的电脑上安装好这一数字证书。

考虑到在具体实现上,签名、加密、解密和验证签名等操作的实现函数每次所能处理的数据的大小一般都会小于整个文件的大小,所以系统将对文件进行分块处理,每次处理文件的一个数据块。譬如在对文件进行数字签名处理时,系统将依次读取文件的每一个数据块来进行数字签名操作,不断循环,直至整个文件处理完毕。对数据块进行签名的流程图如图 2 所示。

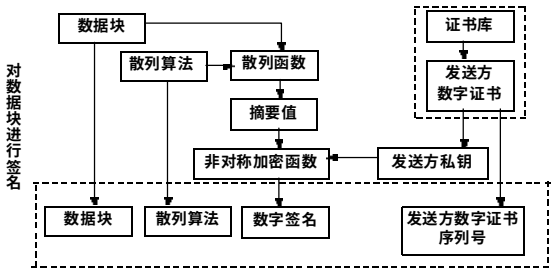

图 2 对数据块进行签名流程

(2)对文件进行加密:根据PKI理论,要对文件进行加密,发送方必须首先取得接收方的公钥,发送方可通过访问公钥基础设施的证书库而查询并下载到接收方的数字证书,接收方的公钥就包含在该证书中,利用这一公钥发送方就可对文件进行加密,而接收方在接收到经加密处理的文件后将用自己的私钥进行解密,然后才能读取文件信息。由于用公钥进行加密处理的数据只有用相应的私钥才能进行解密,而用户的私钥只有用户自己才能获取和使用,所以即使攻击者能在文件信息传输过程中将其截获,也无法对文件信息进行解密,从而无法理解其中的信息,文件的机密性就得到了保证。

同样的,系统将对文件进行分块处理,依次加密每一个文件数据块。对数据块进行加密的流程如图 3 所示。

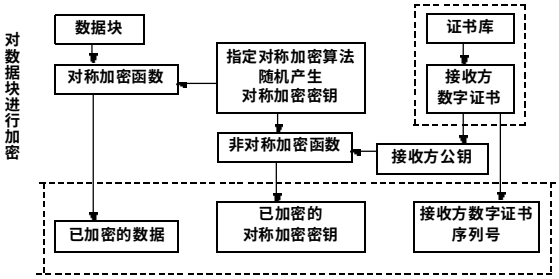

图 3 对数据块进行加密流程

值得一提的是，鉴于非对称加密算法在运行速度上要比对称加密算法慢很多，在对数据块进行加密时结合使用了对称加密技术和非对称加密技术，用对称加密函数对数据块进行加密，并用非对称加密函数对对称密钥进行加密，以求得在增强安全性的同时提高系统的运行效率。相应的，在进行解密时，将首先解密出对称密钥，再用它解密出原始数据块。

(3)对文件进行解密：接收方在接收到经过加密处理的文件之后，必须先进行解密处理才能读取文件信息。对文件进行解密，我们同样要采取分块处理的方式。对文件数据块进行解密的流程如图 4 所示。

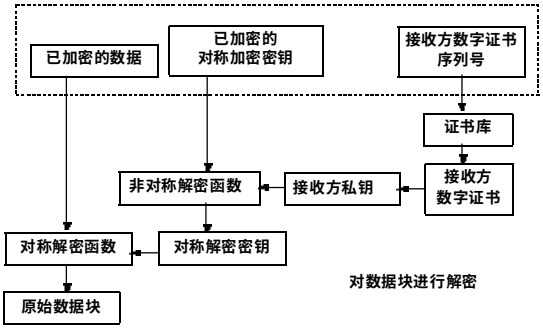

图 4　对数据块进行解密流程

(4)对文件进行验证签名：接收方在接收到经过签名处理的文件之后，必须进行验证签名以判断文件在传输的过程中是否已被篡改以及文件是否确实是由指定的发送方发送过来的，验证无误后才能读取文件信息。对文件进行验证签名，我们同样要采取分块处理的方式。对文件数据块进行验证签名的流程如图 5 所示。

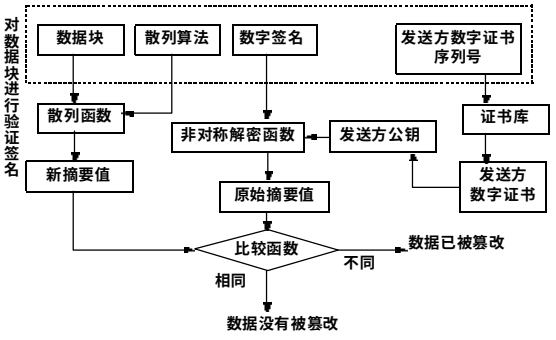

图 5　对数据块进行验证签名流程

3.5　关于文件的传输

对文件进行安全处理之后我们就可以利用系统的网络传输模块将它发送给接收方了，系统的网络传输模块不仅可以发送和接收文件，还可以发送和接收即时消息，这使得用户在传输文件的同时还可以进行点对点的即时交流。系统的网络传输模块是通过 Windows Socket 套接口编程技术来实现的，其核心工作是创建通信双方之间的连接，并利用这一连接传输文件和即时消息。由于在传输数据时我们每次所发送和接收的都是一个个的数据包，所以一个关键的问题是一方如何让对方理解他所发送的数据包中包含的是什么数据，对方只有在知道这一点的情况下才能对数据采取相应的措施。为此，系统为通信双方定义了一个简单的通信协议。

这个协议的关键部分是通信数据包的格式，而该格式主要依赖一个结构体，通信双方在发送数据给对方时都是发送一个个的结构体对象，这个结构体的 C++ 语言定义如下：

```
struct MyPacket
{
    char  head;
    long  part;
    long  dataLen;
    char  data[1010];
};
```

其中 head 用于指出整个数据包的用途，可能是传输文件数据块，也可能是传输即时消息，还可能是传输连接控制消息；part 用于在传输文件数据块时指出所传数据块是整个文件的第几块，它的使用有助于接收方准确无误地接收文件；dataLen 用于指出文件数据块的长度或即时消息数据的长度；data 数组用于存放具体的文件数据块或即时消息数据。依据该结构体就可定义具体的协议内容，规定各种通信数据包的意义，协议定义好后，就可以方便地进行文件的发送和接收以及消息的发送和接收了。双方将严格按照既定协议进行通信，以确保对方能正确解析接收到的数据，实现数据的正确传输。

考虑到系统用户很可能并不处于同一个局域网，而是通过各种方式连接到 Internet，所以为了满足各种用户进行安全文件传输的需求，我们在设计时使系统的安全处理模块和网络传输模块彼此相对独立，使得用户在对文件进行安全处理之后，可以使用系统的网络传输模块来将文件发送给接收方，也可以使用电子邮件、QQ、FTP 软件等各种网络传输工具将文件发送给接收方，接收方接收到文件后再利用系统的安全处理模块进行相应的安全处理即可，这一灵活性使得本系统可以广泛地应用于各种网络之中。

4　结　论

本文分析了安全文件传输系统所要达到的目标，引入了 PKI 机制，利用数字证书来对文件进行数字签名、加密等安全处理，然后通过并不安全的网络通道进行传输，接收方接收到文件后相应地进行解密、验证签名等安全处理而得到原始文件，从而保障了传输的文件的机密性、完整性并验证文件的真实来源，实现文件的安全传输。

参考文献：

[1] Carlisle Adams,Lloyd Steve.公开密钥基础设施——概念、标准和实施[M].北京:人民邮电出版社, 2001.

[2] Nash Andrew,Duane William,Joseph Celia,et al.公钥基础设施(PKI):实现和管理电子安全[M].北京:清华大学出版社, 2002.

[3] Articsoft.Introduction to public key infrastructure[EB/OL].http://www.articsoft.com/wp_pki_intro.htm.

[4] 吉林省数字证书认证中心. PKI 浅析二[EB/OL]. http://www.jlca.com.cn/jlca_5/infocontent.jsp? infoid=144.

[5] Schneier Bruce.应用密码学(协议算法与 C 源程序)[M].北京:机械工业出版社, 2000.

[6] Microsoft.Platform SDK Documentation[CP/DK].Microsoft.