一种企业安全电子邮件系统的设计与实现

张啸农[1],徐向阳[2]

(1. 长沙理工大学 计算机与通信工程学院,湖南 长沙 410076;
2. 湖南大学 计算机与通信学院,湖南 长沙 410082)

摘 要:通过分析现有电子邮件遇到的安全问题,用密码学和安全认证技术来解决这些安全漏洞。在此基础上提出了一种基于PKI的安全电子邮件系统。该系统在邮件收发终端引入智能密码钥匙,保证了重要机密信息的安全传输和存储,有效地解决了现有邮件系统在收发邮件中的安全问题。

关键词:PKI;智能密码钥匙;安全电子邮件系统

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)10-0131-03

Design and Implementation of a Secure E-Mail System in Enterprise

ZHANG Xiao-nong[1], XU Xiang-yang[2]

(1. Coll. of Computer and Communication Eng., Changsha Univ. of Sci. and Techn., Changsha 410076, China;
2. Coll. of Computer and Communication, Hunan Univ., Changsha 410082, China)

Abstract: Analyse the security problems which exsist in current E-mail system. And solve these security problems with the cryptology and the safe authentication technology. In this foundation, propose a kind of security E-mail system which based on the PKI technology. This system uses SecurityKey at the terminal of receiving and dispatching, which guaranteed the important secret information safely transmitted and storage, and it could effectively solve the security problem which exists in current E-mail system of receiving and dispatching the mail.

Key words: PKI; securitykey; secure E-mail systems

0 引 言

电子邮件现已成为最普遍的网络应用,但邮件系统面临许多安全威胁。电子邮件的不安全性有以下几点[1]:

(1)电子邮件在Internet上没有任何保密措施,电子邮件从一个网络传到另一个网络,最终到达目的网络,整个过程中电子邮件都是不加密的可读文件,用户的电子邮件有可能被人偷窥甚至篡改。因此,应保证电子邮件的完整性,即保证电子邮件在传输过程中未被篡改。

(2)他人可轻易地使用冒用的电子邮件地址发送电子邮件,伪造身份从事网络活动。因此要防止他人冒充发信人,通过认证确保邮件的确来自真正的发信人。

(3)电子邮件的发送者还可能抵赖他发送的电子邮件。因此还要提供一定的安全机制,使其具有不可否认性,发信人无法否认他发过去的电子邮件。

由于电子邮件这些不可靠的特点,所以虽然它被广泛地用来进行网络通信,但是真正重要的信息仍然不宜使用电子邮件来传递。

收稿日期:2006-02-14

作者简介:张啸农(1981-),男,湖南长沙人,硕士研究生,研究方向为信息安全;徐向阳,副教授,硕士生导师,研究方向为信息安全、密码学。

针对电子邮件所面临的安全问题,提出了一种基于PKI的安全电子邮件系统,该系统在邮件收发终端引入智能密码钥匙,保证了重要机密信息的保密性和安全性,有效地解决了现有邮件系统收发电子邮件中的安全问题。

1 相关技术

1.1 对称密钥密码体制(Symmetric Key Cryptosystem)

即信息的发送方和接收方用一个密钥去加密和解密数据的密码体制。它的最大优点是加/解密速度快,适合于对大数据量进行加密[2]。

1.2 非对称密钥密码体制(Asymmetric Key Cryptosystem)

也称公钥密码体制,是指信息加密和解密使用两个不同密钥的密码体制。它使用的两个密钥,一个公开发布,即公开密钥(publickey),另一个由用户自己秘密保存,即私用密钥(privatekey)。信息发送者用公开密钥去加密,而信息使用者用私用密钥去解密。公钥机制灵活,具有较好的安全性[2]。

1.3 数字信封

一般来说,并不直接使用非对称密码技术加密明文,而仅用它保护实际加密明文的对称密钥,即所谓的数字信封(Digital Envelope)技术[3]。

1.4 数字签名及数字摘要

数字签名是指用户用自己的私钥对明文的数字摘要(由散列函数产生)进行加密后所得的数据。由于发邮件者的私钥只有他本人才有,所以他一旦完成了签名便保证了发件人无法抵赖曾发过该邮件(不可抵赖性)。经验证无误的签名邮件同时也确保邮件在经签名后未被篡改(完整性)[4]。

1.5 PKI

PKI (Public Key Infrastructure)既公开密钥体系,是为所有的网络应用提供加密和数字签名服务的一种密钥和证书管理体系。它包括数据加密、认证理论、数字签名、密钥管理、证书认证中心系统建设等诸多方面[5]。

1.6 CA 简介

CA 又称为认证中心,它是被用户所信任的签发公钥证书及证书注销列表的管理机构[6]。

1.7 智能密码钥匙

智能密码钥匙也叫 UKEY 或 EKEY,是一种集智能芯片和读写控制于一体的 USB 接口产品,用于存放加密和签名证书,并在 USB KEY 内部实现对信息的加密和签名。

1.8 PCI 密码卡

PCI 密码卡是专门为密码处理和计算而精心设计与优化的硬件设备,它生成非对称密钥、加密证书,并实现签名运算、加密处理。

2 安全电子邮件系统的设计

2.1 系统总体拓扑结构

系统总体拓扑结构如图 1 所示。其中,CA 认证中心对签发公钥证书及证书注销列表进行管理。密钥管理中心负责为通讯用户配发智能密码钥匙 UKEY,并对本系统发放的证书与密钥进行管理、维护。用户在本地客户端 PC 上安装安全邮件系统用户端应用程序,配合智能密码钥匙 UKEY 的使用,就支持用户通过互联网、政府外网以及企业内部网络实现文件的安全交换与管理。

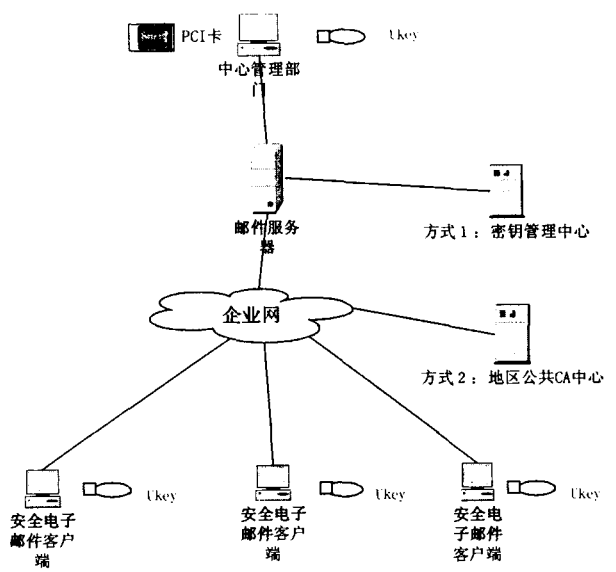

图 1 系统拓扑结构

2.2 系统安全性设计

(1)密钥管理安全。

系统建立的密钥管理中心,负责数字证书及密钥的管理。系统所使用的密钥是由高速密码卡生成。根密钥存放在 PCI 密码卡里,根密钥对的公钥经系统签名,而生成自签名证书。

所使用的密钥包括签名证书和加密证书的两对非对称密码算法的公、私钥对,以及对称密码算法的密钥两种类型。

用户申请加密证书和签名证书,密钥管理中心签发证书后,将证书和密钥导入安全智能密码钥匙 SecurityKey 中,用户修改 PIN 码后颁发给用户。其中加密证书的私钥在数据库中有备份,而签名证书的私钥由用户的密码钥匙产生并存放。

(2)加解密过程的安全。

加密操作和签名操作都在专用硬件设备中完成,系统将数据准备好后,将其送到密码卡内进行处理,处理完毕,再将结果返回。整个加解密和签名过程中,关键信息不会泄露到内存中。

(3)身份认证安全。

通过系统的证书系统实现身份认证,应用 PKI 机制实现对使用者身份的认证,高强度的密码加密技术保障了身份认证的安全性。

(4)操作权限的身份认证。

电子邮件进行加密时,其密钥是由 SecurityKey 自身随机产生的,该密钥用接收方的加密公钥进行加密。接收方必须用自己的 SecurityKey 中加密私钥才能打开文件,获得相应权限,进行相应的操作。也就是说没有相关操作权限的人就无法打开文件或进行其他操作。

(5)文件存储的安全性实现。

文件采用特殊的安全存储机制,文件系统管理由自身进程处理,不被外部进程所截获,保证安全加密文件在本地处理过程中的安全性。系统自建的安全文件夹,为文件存储提供了完善的安全保护机制。安全文件夹的处理功能必须在通过 SecurityKey 的身份认证后,才能启动。

2.3 系统模块组成

系统基本组件包括:PCI 密码卡、智能密码钥匙、密钥管理中心、安全电子邮件系统、安全文件夹系统等。总体模块结构如图 2 所示。

其中,安全文件夹系统采用加密和数字签名相结合的方法,实现用户 PC 端的数据文件存储保护[7]。它对进入安全文件夹的文件自动进行加密保护,防止文件被非法窃取、破坏、伪造或修改。用户必须插上合法有效的智能密码钥匙,才能查看、操作与管理安全文件夹。粉碎机则实现完全不可恢复的文件数据清除,保证重要机密数据的安全。

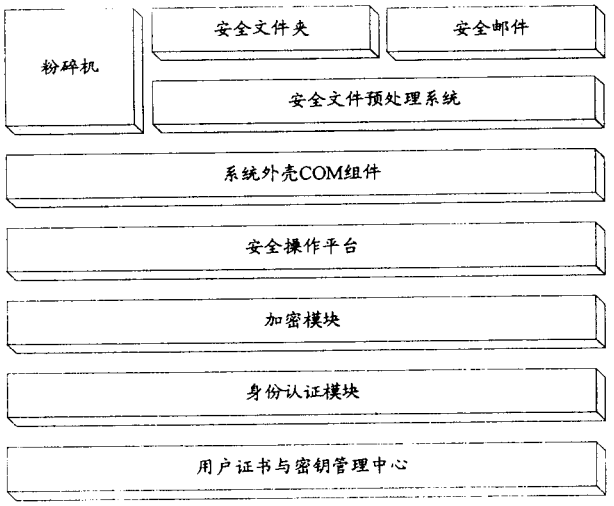

图 2　系统总体结构

2.4　安全电子邮件系统的模块设计

安全电子邮件系统以数字证书为基础,采用数字签名、数字信封、规则检验、访问控制等技术来保证信息的保密性、完整性、可用性和不可否认性,为网络上信息传输的安全、保密提供有力保障。该系统的功能模块组成如图 3 所示。

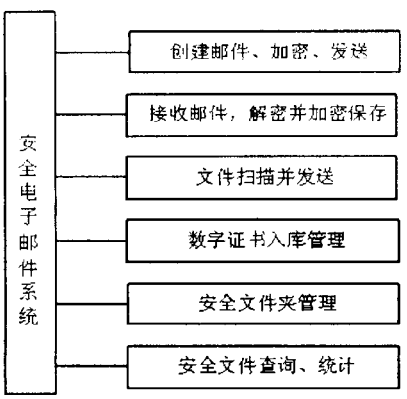

图 3　系统功能模块组成

(1)创建邮件、加密与发送模块功能是:建立一个界面,用来显示创建文件、邮件、显示与编辑;支持附件拖动放入界面,并将附件在附件框中列表显示;支持用户加入多个系统证书列表中的用户地址;签名和加密要发送的邮件或文件;签名和加密完成后保存到所设定的目录;最后将签名和加密的邮件或文件,发送到指定的邮件接收方。

(2)接收邮件、解密并加密保存功能是:将收到的签名与加密的邮件或文件进行验证签名和解密处理,并把明文显示出来,便于阅读和打印;支持利用安全文件夹管理功能,将明文加密存储到安全文件夹中。

(3)文件扫描、发送功能是:支持多种类型的扫描仪,将纸质文件利用扫描仪扫描成指定文件名的图片文件,然后对其加密处理,之后利用邮件发送功能,将文件发送给指定的接收者。

(4)证书入库(安全邮件地址簿)管理功能是:自动将用户证书列表更新(包含证书的注销、增加、修改后的证书列表),以保证用户安全邮件地址簿的有效性。当密钥管理中心对证书进行修改后,将发送密钥给最近改动的用户,同时发送证书库给所有已注册的用户。用户收到密钥管理中心发送的安全邮件后,如果判定为证书库,则在验证签名后,自动更新证书库(安全邮件地址簿)。

(5)安全文件夹管理功能是:增加、删除、更名文件夹;支持多级文件夹;支持将用户的文件、邮件存放在安全文件夹中;支持显示所有文件列表;支持预览文件标题与附件名称;支持打开安全文件;支持在不同文件夹中移动安全文件;支持安全文件、文件夹属性设置与查看等。

(6)安全文件查询、统计功能是在整个安全文件夹或者指定的目录下,依照发送人地址、接收人地址、创建时间、文件标题、是否为接收的邮件等结合模糊查找安全文件,并进行统计。

3　安全邮件系统主要控制流程

3.1　生成用户证书和密钥

首先在密钥管理中心生成用户的加密证书和签名证书。加密证书用来加密邮件的内容,当别的用户要给该证书持有人发送安全邮件的时候,他需要得到该加密证书;签名证书用来保证证书所有人发送信息的完整性,用户要

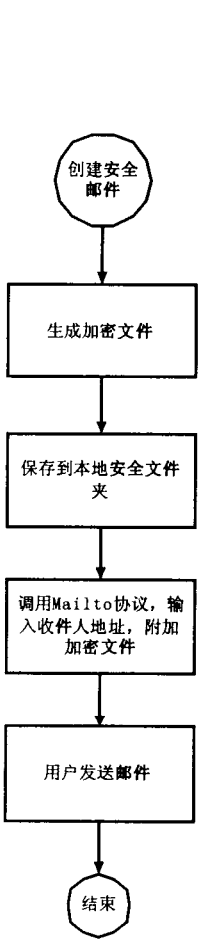

图 4　创建邮件、加密并发送流程

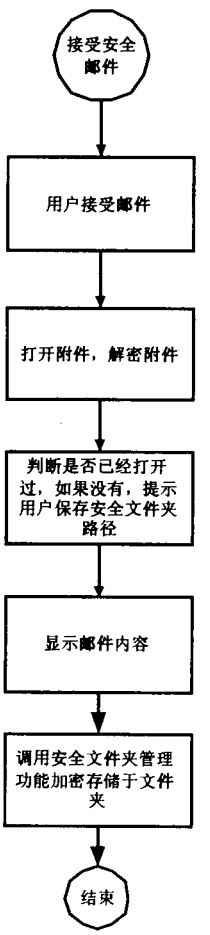

图 5　接收邮件、解密,并加密保存流程

(下转第 136 页)

用户密钥 Key。

3 安全性分析

该方案的安全性依赖于具体所选用的相关安全算法的安全性[4],故在实现时必须选用安全性较强的算法,例如哈希算法可以选择 SHA-1,对称加密算法选择 IDEA 或 AES。恢复密钥时需要使用用户预注册的私密性问题对发出密钥恢复请求的用户进行身份验证,所以必须由用户本人独立地注册这些问题,其他任何人不得参与[5]。

构造外部密钥恢复块的主要目的是在不泄漏密钥信息给 keyServer 的前提下,让其充当中间人,对请求者进行身份验证。用户传给 keyServer 的 symKey_B_1 - symKey_B_r 仅仅能够判断这个用户是否是合法用户,即密钥的主人。若用户可以证明自己有能力生成 symKey_B_1 - symKey_B_r,那么用户同样可以生成 symKey_A_1 - symKey_A_r。因为必须使用 symKey_A_1 - symKey_A_r 才能解出在内部恢复块(innerBlock)中的 encKey,而由 symKey_B_1 - symKey_B_r 推导不出 symKey_A_1 - symKey_A_r,所以 keyServer 无法得知用户存储的密钥。

若密钥恢复阶段在用户和 keyServer 之间存在攻击者,攻击者可能会通过监听网络数据包取得 symKey_B_1 - symKey_B_r 或内部恢复块,但由于哈希算法本身所具有的单向不可逆性以及在建立内、外部密钥恢复块的过程中使用了不同的魔数(magic1,magic2),使得攻击者无法根据 symKey_B_1 - symKey_B_r 的值推导出问题的答案或者 symKey_A_1 - symKey_A_r。除非攻击者能像密钥主人一样正确回答至少 r 个私密问题,否则攻击者只能按图 2 的流程得到一个假密钥,同时由于 shares_B_i,shares_A_i 等同于一些随机数,攻击者无法根据结果判断答案的对错,增大了破解的难度。

4 结束语

综上所述,文中综合应用哈希算法、对称加密技术、门限原理,结合易于使用的回答问题认证模式,提出了一套密钥恢复新方案。该方案不仅适用于对用户密钥、口令进行保存以及恢复,还可用以对其他私密信息进行类似处理,具有一定的通用性。

参考文献:

[1] Blakley G R. Safeguarding Cryptographic Keys[A]. Proceedings of AFIPS 1979 National Computer Conference[C]. Zürich, Switzerland: [s. n.], 1979.

[2] Shamir A. How to share a secret[A]. In Communications of the ACM[C]. Boston, America: [s. n.], 1979.

[3] Price W. A PGP Corporation White Paper: inside PGP Key Reconstruction[EB/OL]. http://www.pgp.com/support/wp1.html, 2003.

[4] Trappe W, Washington L C. 密码学概论[M]. 许鹏文,等译. 北京:人民教育出版社,2004.

[5] Hsu C L, Wu T C. Authenticated encryption scheme with (t, n) shared verification[A]. IEEE Proceedings Computer Digital Techniques[C]. Oatarom, Canada: [s. n.], 1998.

(上接第 133 页)

验证接受的邮件是否完整可信的时候,需要获得此证书。然后由 PCI 卡生成加密密钥,注入到用户的 UKEY 中,并且在密钥管理中心系统中保留备份,签名密钥由用户的 UKEY 自己产生,并且不被密钥管理中心中心备份,这样可以保证用户签名私钥的惟一性,以支持用户签名的不可否认性。接着给该证书用户发送根证书、签名证书以及最新的证书库;所有的证书最后封装为一封安全邮件发送给该用户;最后系统给所有合法的用户发送最新的证书库,以保证各个邮件客户端的证书库实时更新,确保数据的一致性,使系统能正常运行。

3.2 创建、加密并发送安全电子邮件

创建邮件、加密并发送流程见图 4。

3.3 接收、解密并加密保存安全电子邮件

接收邮件、解密,并加密保存流程见图 5。

4 结 论

该系统通过建立统一的密钥管理中心来建立基本的信息安全保护体系,还建立了用户端的安全文件管理与传输系统,实现文件的安全存储管理、文件加密管理、身份认证、数字签名等功能;同时也建立文件交换机制,实现电子邮件的加密传递,保证邮件的机密性、完整性和不可否认性;实现了本地机密文件的加密存储机制,以及机密文件删除后不可恢复机制。因此本系统具有安全性高的特点,为政府和企业安全收发包含重要文件的电子邮件提供了很好的解决方案和安全保障。

参考文献:

[1] 胡 珊,顾其威. 企业电子邮件系统安全性技术研究及实现[J]. 小型微型计算机系统,2003(1):157-159.

[2] 施奈尔. 应用密码学——协议、算法和 C 源程序[M]. 北京:机械工业出版社,2001.

[3] Burnett S, Paine S. 密码工程实践指南[J]. 冯登国译. 北京:清华大学出版社,2001.

[4] Steve G A. 公开密钥基础设施——概念、标准和实施[M]. 冯登国译. 北京:邮电出版社,2001.

[5] 关振胜. 公钥基础设施 PKI 与认证机构 CA[M]. 北京:电子工业出版社,2002.

[6] 徐志大,南相浩. 认证中心理论与开发技术[J]. 计算机工程与应用,2000,36(9):87-90.

[7] 卢大航. 超大容量商用邮件系统的设计与实现[J]. 计算机应用研究, 2001,18(11):93-95.