基于服务器端安全电子邮件系统的设计与实现*)

姚伏天　金连甫　潘　敏
(浙江大学计算机科学与工程学院　杭州310027)

摘　要　电子邮件作为Internet网络的重要应用，其安全性能越来越受到重视。本文针对目前基于客户端软件的安全电子邮件系统的一些不足，结合目前比较成熟的加密与数字签名技术，提出了在邮件服务器端实现邮件安全性的新思路，设计和实现了基于局域网服务器端安全电子邮件系统(SESICS)，并且对SESICS系统进行了安全评估。

关键词　数字证书，数字签名，邮件服务器，安全性

The Design and Implementation for Secure Email System Based on Intranet Computer Server

YAO Fu-Tian　JIN Lian-Fu　PAN Min
(Department of Computer Science and Engineering, Zhejiang University, Hangzhou 310027)

Abstract　As an important application of Internet, the electronic mail should be secured well. According to the deficiency of security email system which is based on computer client, combined with the technology of Cryptography and Digital Signature, the paper raises a new method of achieving the email security on Intranet email server, and puts forward a design and implementation for Security Email System Based on Intranet Computer Server (SESICS), and at last gives a security evaluation to this system.

Keywords　Digital certificate, Digital signature, Electronic mail server, Security

1　引言

电子邮件是目前Internet用户最常用的服务，因为它高速、方便、快捷，不要求交流双方同时在线，电子邮件正在成为传真、电话、普通信件以外的一种全新的交流沟通工具。但是由于互联网环境的开放特点，普通电子邮件的通信又存在着安全问题，主要表现在：

(1)信息泄漏：电子邮件在存储转发的过程中容易被第三者非法截获。如果电子邮件以明文的形式存在，邮件中的个人隐私或商业机密就会在第三者面前暴露无疑。

(2)信息篡改：发信方发给接收方的信件被第三者截获后，可能会被第三者修改后再发往接收方。

(3)假冒身份：非法者可能会伪造信件，假冒某一用户的身份向其他用户发送电子邮件。

(4)抵赖：发送方否认曾经向接收方发送过某一内容的信件。

电子邮件的安全性包括保密性，认证身份，数据完整性和不可否认性等四个方面。在现阶段，一些基于客户端软件的安全电子邮件系统已经投入使用。这种方法实现简单方便，目前已经在某些情况下起到了保护电子邮件的作用。

然而对于在局域网内的所有计算机而言，基于客户端的安全电子邮件系统实施起来比较困难，而且成本比较高。由于局域网内的所有电子邮件的传递和分发都要经过邮件服务器，本文提出了实施方便而且成本较低的基于局域网服务器端的安全电子邮件系统(SESICS)。

本文首先介绍了保障邮件系统安全的技术背景，分析了目前局域网内的安全电子邮件系统的特点和不足，接着阐述了SESICS系统的设计思想和详细流程，并对SESICS系统进行了安全性能的评估，最后提出了该系统的前景展望。

2　技术背景

2.1　加密技术

对发送的邮件的内容进行加密，保证邮件的内容在传输过程中不被泄露是安全电子邮件系统的一个基本功能。而其中加密算法的选择是决定邮件加密强度与效率的一个重要方面。基本的加密算法有两种：对称密钥加密，非对称密钥加密。对称密钥加密也叫秘密密钥加密，即发送和接收数据的双方必须使用相同的，对称的密钥对明文进行加密和解密运算。非对称密钥也叫公开密钥加密算法，它主要指每个人都有一对唯一对应的密钥：公开密钥和私有密钥，公开密钥对外公开，私有密钥个人秘密保存：用其中一把密钥来加密，就只能用另一把密钥来解密。

信息摘要算法MD5，全称是Message-Digest Algorithm，其作用是让大容量信息在用数字签名软件签署私人密钥前被"压缩"成一种保密的格式。MD5的典型应用是对一段信息(Message)产生信息摘要(Message-Digest)，以防止被篡改。

2.2　数字证书

数字证书(又称数字标识)是用于证明电子邮件用户身份的一种技术方式，是允许电子邮件用户在如电子交易中提供身份证明的、独一无二的特殊文档。它由发证机构发布给它认可的个人或组织，用于数字签名的某些信息使用户可以通过这些信息确认其作者，或用作加密信息以防止其它人查看。

*)基金项目：浙江省自然科学基金重点项目(ZD0225)；浙江省自然科学基金(601157)。**姚伏天**　硕士研究生，主要研究方向：计算机网络和通信技术，网络与信息安全技术；**金连甫**　教授，主要研究方向：计算机网络和通信技术；**潘　敏**　硕士研究生，主要研究方向：计算机网络和通信技术，无线网络应用。

数字证书由公用密钥、私人密钥和数字签名三部分组成。公用密钥是提供给他人、以便他们给你发送加密邮件(即为确保邮件的内容只能被目标收件人阅读而将邮件内容改为数字代码的一种邮件)的数字证书组成部分。对所发邮件进行加密有助于确保只有预定接受人员才能在传送过程中读取该邮件。私人密钥是数字证书中只供你自己用来对加密邮件进行解密和阅读的部分。数字签名是你的电子身份卡,通过数字签名,你可在所发电子邮件上签署独特的标识,这样收件人就可以确认邮件是你发送的,并且邮件在传送过程中未被伪造或篡改。

正是由于数字证书的这三个各有分工的组成部分,才允许用户签发电子邮件,使目标收件人可以确认经数字签名的邮件确实由用户发送的,并且未被篡改,同时,才允许他人向用户发送加密邮件。也就是说,数字证书允许用户证明自己在Internet上的身份,这与人们日常生活中所用的其它ID卡功能极其相似。

安全电子邮件是通过数字证书对电子邮件的特殊作用来实现的,通过数字证书,安全电子邮件具有了一般电子邮件所不具备的安全特征。具体体现在:

1. 保密性:通过使用收件人的数字证书对电子邮件加密(这里用到了加密技术)。加密后,只有收件人才能阅读加密的邮件。这样,在Internet上传递的电子邮件信息将不会被人窃取,即使发错邮件,收件人也无法看到邮件内容。

2. 认证身份:在Internet上传递电子邮件的双方互相不能见面,所以必须有方法确定对方的身份。利用发件人数字证书在传送前对电子邮件进行数字签名,便可确定发件人身份,而不是他人冒充的。

3. 完整性:利用发件人数字证书在传送前对电子邮件进行数字签名不仅可确定发件人身份,而且传递的电子邮件信息也不能被人在传输过程中修改。

4. 不可否认性:由于发件人的数字证书只有发件人唯一拥有,故发件人利用其数字证书在传送前如果对电子邮件进行了数字签名,发件人就无法否认发过这个电子邮件。

3 基于客户端软件的安全电子邮件系统

在Microsoft的Outlook Express中,已经实现了用加密技术和数字证书来保障电子邮件的安全。其原理是:当用户发送电子邮件时,先要去某CA中心下载并安装该CA中心发布的数字证书。然后用该证书中包含的密钥对电子邮件进行加密;当用户接收邮件时,收件人也要选择相应公司发布的数字证书,然后将对应的密钥对电子邮件进行解密工作,从而读取邮件原始的文档。

流程如图1所示。

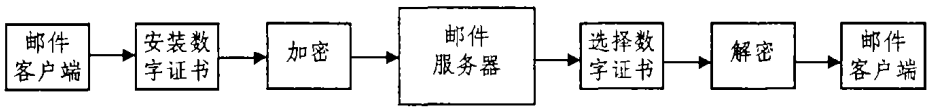

图1 基于客户端软件的安全电子邮件流程

4 基于客户端软件的安全电子邮件系统的一些不足

然而,对局域网内的所有计算机而言,目前这种基于客户端软件的电子邮件安全系统并不能理想地发挥作用,存在一些问题和不足。

1. 电子邮件的客户端软件种类很多,局域网内的用户往往使用多种不同的电子邮件客户端软件。但目前来说,除去Outlook Express和有限的几个客户端软件外,其他的客户端软件均不提供数字证书功能,故对那些使用其他客户端软件的用户来说,其电子邮件的安全性就得不到保障。而那些用惯了某种邮件客户端软件的用户往往不愿意更换其客户端软件。对于大型的局域网内的计算机,统一更换客户端软件实施起来难度很大。另外,大量的用户使用局域网内部webmail来收发邮件。而webmail目前也不能提供数字证书服务,同样,局域网内部webmail用户也无法安全的收发电子邮件。

2. 许多提供数字证书的CA中心本身为商业机构,它们以盈利为目的。其数字证书不是免费的,在试用了一段时间后(通常为三个月),用户就要为购买数字证书交纳一定费用。另外,为了保证安全性,数字证书经过一定时间后就得作废,用户需要购买新的证书。对局域网内的用户来说,如果每个局域网用户都去购买数字证书,那累计起来就是一笔非常大的费用,这将增加局域网的运营成本。

对于局域网内的计算机来说,由于有网络管理员控制,在局域网内收发邮件并不要考虑太多的安全因素。然而,一旦局域网连接到Internet,而Internet上存在恶意用户和黑客的攻击,故局域网内计算机向局域网外收发邮件时安全性能就马上显得格外重要。于是,一种安全性能好,实施简单,成本低廉的局域网安全电子邮件系统成为许多局域网组织的迫切需求。

5 基于局域网服务器端的安全电子邮件系统模型的设计与分析

针对以上情况,本文提出并设计实现了基于局域网服务器端的安全电子邮件系统模型。

5.1 基本思路

某一局域网组织(公司,学校,机关)作为一个单位购买获得数字证书,数字证书的安装、选择和电子邮件的加密、解密都在该局域网的邮件服务器上进行,对局域网内用户是透明的。即局域网内用户不需要单独购买和安装数字证书,可以使用各种电子邮件客户端软件,或者采用局域网内的webmail,仍按照原先的方式收发未加密的电子邮件,发送和接受邮件就可以得到良好的安全性能。

邮件服务器的基本组成包括:邮件分发代理(Mail Delivery Agent,MDA),邮件传送代理(Mail Transfer Agent,MTA),邮件用户代理(Mail User Agent,MUA)。

MDA只关注发往本地邮件服务器上用户的邮件信息,它从MTA程序接收邮件,然后决定怎么样分发这些邮件。

MTA负责处理所有接收和发送的邮件。对于每一个外发的邮件,MTA决定接收方的目的地。如果目的地就是本机,MTA将邮件交给MDA进行投递。

MUA向用户提供了读取存在他们邮箱中邮件的操作界

面。

为使基于局域网服务器端的安全电子邮件系统(SESICS)具有可扩充性,其设计方案为:在邮件服务器中增加一个邮件操作代理(MOA:Mail Operate Agent),集成入MTA中,与MTA,MDA,MUA一起协同工作。结构见图2。

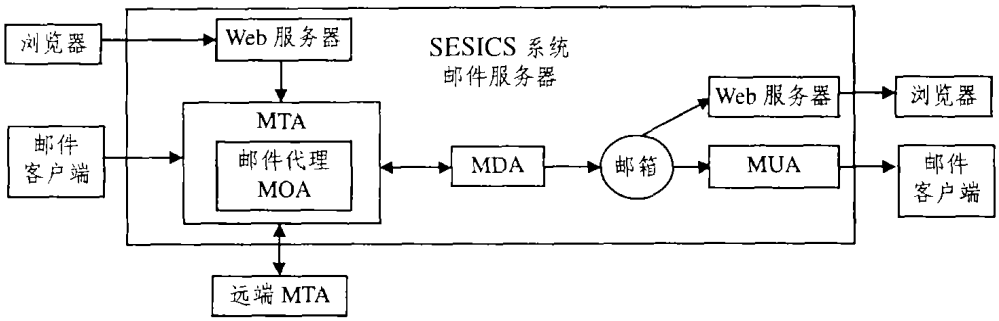

图2 SESICS系统的工作原理结构图

5.2 SESICS系统的主要流程

SESICS系统中的邮件操作代理MOA主要分为三个流程:数字证书流程,邮件发送流程和邮件接收流程。

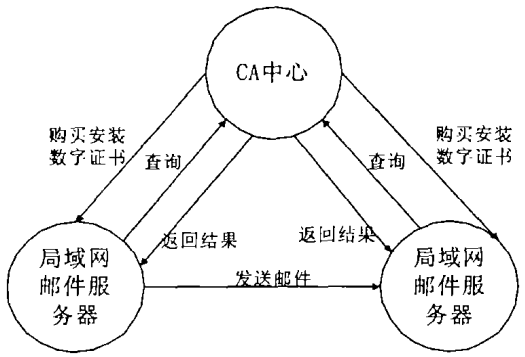

图3 SESICS系统的数字证书流程

5.2.1 数字证书流程 局域网组织购买并安装数字证书,得到一对密钥(公用密钥和私人密钥),由该局域网的网络管理员保管,局域网的普通用户得不到访问的权限。发送邮件和接收邮件时,系统会连接到CA中心查找对方的数字证书,从而得到对方的公钥。为了和那些没有安全性功能的邮件服务器相兼容,SESICS系统收发邮件有两种方式:安全方式和普通方式。如果在CA中心查到对方的数字证书,就采用安全方式,否则,采用普通方式,没有安全性措施,邮件的安全性得不到保障。

5.2.2 邮件发送流程 局域网用户将电子邮件明文发送到SESICS系统邮件服务器中的MOA。MOA对原始邮件启动加密程序。首先解析得到电子邮件的收件人和发件人,然后到CA中心查得该邮件收件人的公钥,从安装的数字证书得到发件人的私钥。用MD5消息摘要算法计算信件明文得到邮件摘要,用发件人的私钥RSA加密邮件摘要得到加密摘要。接着将信件明文进行压缩,并且由随机数得到128位会话密钥,用会话密钥IDEA加密压缩信件得到密文文件。再将会话密钥用收件人公钥RSA加密得到加密后的会话密钥,这样就生成了数字信封和数字签名。最后将加密后的会话密钥、密文文件和加密摘要三者合成起来就形成了在Internet上传输的密钥密件(见图4)。

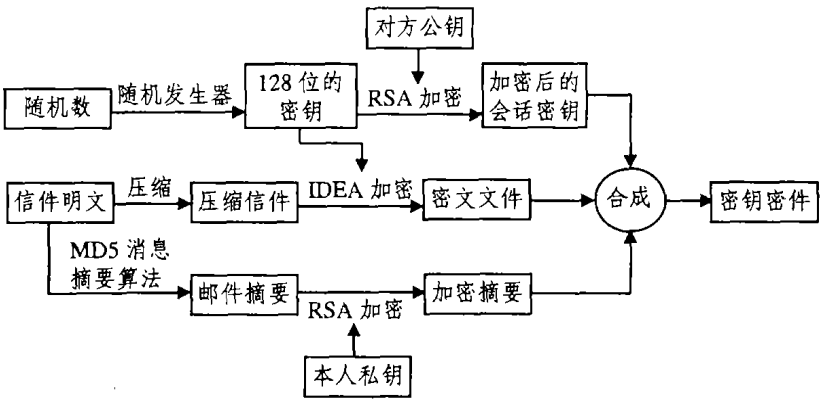

图4 SESICS系统的加密流程

5.2.3 邮件接收流程 当邮件服务器接收到邮件后,首先将密钥密件分解为密文文件、加密密钥和加密摘要。从邮件头可以得知该邮件的发件人和收件人,从安装的数字证书可以得到收件人(本地)的私钥,从CA中心可以得到发件人(对方)的公钥。用自己的私钥RSA解密加密密钥得到128位的会话密钥。然后用会话密钥将密文文件解密得到压缩邮件,将压缩邮件反压缩就可得到信件明文。同时用对方公钥RSA解密加密摘要得到邮件摘要。将邮件原始明文进行MD5计算得到邮件摘要,然后把计算得到的邮件摘要值与接收得到的邮件摘要值进行比较,如果两者一致,则表明邮件在传递过程中,没有经过篡改;否则,说明该邮件已经被篡改过,邮件服务器发出警告,并将该邮件删除(见图5)。另外,当邮件服务器收到邮件后,就给发信人发送一封邮件回执信。如果邮件服务器收到的是回执信,将不再发送回执的回执。

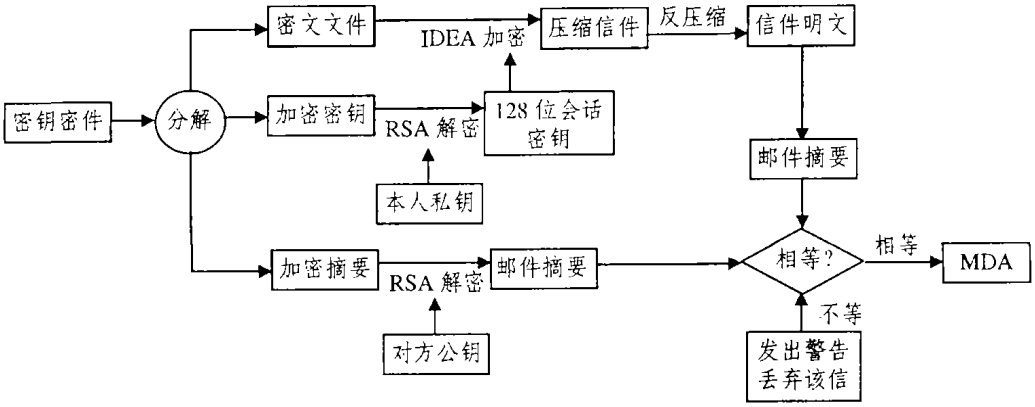

图5 SESICS 系统的解密流程

5.3 SESICS 系统的技术实现

5.3.1 *加密解密* 对称密钥常用的是 IDEA 算法。非对称加密算法常用的是 RSA。两种加密算法各有优缺点。IDEA 加密算法的优点是数学运算量小，加密速度快，但是它的主要缺点是密钥管理困难，密钥的传递渠道解决不了安全性问题，不适合网络环境邮件加密的需要。而 RSA 正好弥补了 IDEA 的缺点，但是具有加密和解密速度慢的缺点。将 RSA 公钥体系的方案和传统对称加密体系的高速度结合起来，可以实现高速有效的加密解密解决方案。

5.3.2 *数字签名的消息摘要实现* 信息摘要算法 MD5，MD5将整个文件当作一个大文本信息，通过其不可逆的字符串变换算法，产生了这个唯一的 MD5信息摘要。如果在以后传播这个文件的过程中，无论文件的内容发生了任何形式的改变(包括人为修改或者下载过程中线路不稳定引起的传输错误等)，只要对这个文件重新计算 MD5时就会发现信息摘要不相同，由此可以确定得到的只是一个不正确的文件。再加上一个第三方的 CA 认证中心，用 MD5还可以防止文件作者的"抵赖"，这就是所谓的数字签名应用。

5.3.3 *开发工具与应用方式* SESICS 系统由纯软件方式实现，在 Windows 操作系统下，用 Visual C++开发平台开发，在 Linux 操作系统下，采用标准 C 开发。SESICS 的主要组成为 MOA 模块，系统设计成外挂模式，提供了 Windows 和 Linux 环境下的不同接口，可以方便地嵌入到目前流行的邮件服务器软件(如 Microsoft Exchanger 和 sendmail，qmail)中。另外，SESICS 系统也可以和一些第3方邮件服务系统实现连接。

6 SESICS 系统的安全性评估

本文从电子邮件安全性的四个方面，对于基于局域网服务器端的安全电子邮件系统(SESICS)进行了评估：

1. 保密性：该系统在局域网的邮件服务器端对邮件进行加密后发送，在 Internet 上邮件以加密形式传递，只有正确收件人经过解密后才能阅读。这样，公网上的黑客或者发错邮件时的收件人无法看到邮件内容。在局域网内部，从客户端到邮件服务器和从邮件服务器到客户端，邮件都是以明文方式传输，可以通过完备的系统日志记录和审计功能来加以防范，内部黑客和发错邮件时的收件人偷看邮件的内容。

2. 认证身份：通过 SESICS 系统向局域网外 Internet 发的电子邮件都用数字证书带有发信人的数字签名，可以为收件人判断确认发件人(或局域网组织)身份；局域网内部的电子邮件，没有附加发件人的数字签名，收件人一般情况下无法确认发件人，但在必要情况下可以通过向系统管理员调查服务器的系统日志记录(如 IP 地址)来确认发件人。发信人必须经过才能登陆 SESICS 系统发送电子邮件，可以防止局域网内冒充他人向局域网外发信。同时，系统管理员可以通过查看系统日志记录来发现局域网内冒充他人发信的情况。

3. 完整性：无论是局域网内邮件还是局域网外邮件，到达邮件服务器后，都被附加上用数字证书加密的邮件摘要，可以保证在传输过程中电子电子邮件信息也不被修改。

4. 不可否认性：通过 SESICS 系统向局域网外 Internet 发的电子邮件带有发信方的数字签名，收件人可以判断发信人是谁，或者来自哪个局域网组织。同时，SESICS 系统自动生成带有收件方数字签名的回执信，发信方可以验证收信方的身份，这样就可以防止双方的抵赖。对于局域网内部邮件，不含有数字签名，必要时可通过系统管理员检查系统日志来防止收发邮件双方的抵赖。

综上所述，在电子邮件安全性的各个方面，基于局域网服务器端的安全电子邮件系统 SESICS 都提供了有力的保障。对于局域网内的所有计算机收发邮件，SESICS 是一个理想的安全保障系统。

结论与展望 保障电子邮件的安全性对于某些局域网组织(如企业，机关单位，学校)有着重要的意义。基于局域网服务器端的安全电子邮件系统 SESICS 安全性能好，而且实施简单，成本低廉。经实践检验，本系统可以方便地与 Microsoft Exchanger 集成，安全性好，目前已经在一些 IT 企业投入试运行，系统稳定，效果良好；由于所有邮件的加密解密和数字证书、数字签名的运算都在邮件服务器上运行，故对服务器配置要求比较高，但相比与当前的邮件系统来说，仍然是一种性价比高的解决方案，是局域网用户实现电子邮件安全性的理想选择。本系统预计未来可以作为局域网内保障电子邮件安全性的一种新的解决思路。

参 考 文 献

1 Schneier B 著，吴世忠等 译. 应用密码学. 北京：机械工业出版社，2000

2 Yang C-H，Yen S-L，Liu K D. Secure official document mail systems for office automation. 0-7803-3913-4-9/97/$4.00 @1997 IEEE

3 Blum R 著，杜鹏 译. 开放源码邮件系统安全. 北京：人民邮电出版社，2002

4 RFC 2015 - MIME Security with Pretty Good Privacy (PGP)

5 Schneier B. E-mail Security New York：John Wily，1995

6 PKCS#1：RSA Encryption Standard，Version 1.4. RSA Data Security，Inc.，1991-06