

对电子邮件加密技术的分析与研究

张瑞丽, 杨坤伟, 李吉亮

(陕西师范大学 计算机科学学院, 陕西 西安 710062)

摘要:随着互联网的发展,电子邮件以其低廉的价格和快捷的速度,越来越受到人们的青睐。然而,与此同时,电子邮件能否安全抵达对方成为人们关心的问题,电子邮件泄密所造成的后果也困扰着人们,因此对电子邮件进行加密处理就尤为重要。文中主要针对电子邮件泄密的问题,详细阐述了对电子邮件加密的四种方法,并分析比较了这些方法的优缺点,对其中存在的问题和挑战进行了研究。

关键词:电子邮件;泄密;加密方法;安全性

中图分类号:TP393.08

文献标识码:A

文章编号:1673-629X(2014)01-0155-03

doi:10.3969/j.issn.1673-629X.2014.01.040

Analysis and Research of Electronic Mail Encryption Technology

ZHANG Rui-li, YANG Kun-wei, LI Ji-liang

(School of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

Abstract: With the development of the Internet, E-mail with its low price and fast speed, get the favor of people. However, at the same time, whether the E-mail can arrive safely becomes a matter of concern to people, consequences of E-mail leaks also bother people, so for E-mail encryption is particularly important. It mainly aims at the problem of E-mail leaks, elaborates the four methods of E-mail encryption in detail, and compares the advantages and disadvantages of these methods, analyzes and studies the problems and challenges.

Key words: E-mail; leak; encryption method; security

0 引言

据一项调查显示,有80%的企业和个人担忧电子邮件沦为泄密管道,致使机密资料误入他人之手,导致整个公司或是个人蒙羞,甚至造成巨大经济损失。有些电子邮件关系到国家机密等信息,泄密后造成的后果不堪设想,当然,这种担忧绝对不是空穴来风,像一些企事业单位的财务报表、商务合同、科研成果、专利技术、市场策略、销售数据等攸关企业自身生存和发展的机密数据,通过电子邮件泄露出去从而造成巨大损失的例子不在少数,法院也受理了不少此类案件。由此可见电子邮件已成为当前企业信息泄密的重要途径,那么保护它的数据安全性就非常重要,其安全防护将是势在必行。那么,在网络的虚拟世界里,工作中通过电子邮件传送的数据信息、生活中通过电子邮件传递的情感以及个人照片,等等,这些文件的保密性由谁来捍卫?随着计算机的发展,对电子邮件的保护也越来越全面,其核心思想是加密处理电子邮件,通过此方

法,允许特定的人对其阅读,从而保证信息的安全性^[1]。所以可以期待网络安全时代的到来,那时会拥有更完善的话语权和隐私权。

1 研究背景

电子邮件面临的泄密威胁^[2]有以下几种方式:

(1)在Internet中,如果电子邮件没有进行任何加密处理,那么它从一个地点到另一个地点,最后到达目的网络,在整个过程中电子邮件都是公开传输,用户的邮件信息就有可能被别人窃取,例如:账单、商务合同等重要信息容易丢失;

(2)在不安全网络中,非法分子只需要修改计算机的一些配置就可冒用你的电子邮件地址轻松地发送邮件,在你毫不知情的情况下,在网络中肆意活动;

(3)当发错电子邮件给不希望发的人或陌生人时,若电子邮件并未经过加密,收件人轻易看到邮件内容,甚者滥用此发错的邮件继续从事网上活动;

收稿日期:2013-03-27

修回日期:2013-05-28

网络出版时间:2013-11-12

基金项目:陕西省科技攻关计划项目(2008K01-58)

作者简介:张瑞丽(1989-),女,硕士,研究方向为密码学与信息安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20131112.1653.051.html>

(4)发送方不承认向接收方发送过某一信件即对自己的行为抵赖。

2 电子邮件加密技术

2.1 对称加密技术

对称加密算法,又称为单密钥算法或秘密密钥算法^[3],顾名思义,使用相同的密钥进行加密和解密。这种算法中,发送方使用加密密钥对原始数据(称之为明文)进行加密之后,把它变成第三方无法看懂的复杂信息(称之为密文)发送至接收方,接收方如果想看到原始数据,根据对称加密技术的原理,他必须通过此加密算法的逆运算对密文进行解密运算,从而变成可读的明文。这种算法是较早应用、技术非常成熟的一种加密算法,但是这种方法存在着严重的不足:

(1)由于接收方和发送方使用相同的密钥,一旦密钥泄漏,那么任何人都能够轻而易举地解密消息;

(2)为了保证安全性,每次使用对称加密算法时,收发双方都需要使用其他人不知道的唯一密钥,这将造成双方所持有密钥的数量以几何级数快速增长,使得密钥管理极其复杂。

因此,针对对称密钥技术的这些不足之处,非对称密钥体系加密技术逐渐产生并成熟,大面积地取代了原来的对称密钥技术。

2.2 传统非对称密钥体系(PKI/CA)加密技术

PKI(Public Key Infrastructure)是指公钥基础设施,它从技术上解决了网络通信安全的种种障碍。CA(Certificate Authority)是指认证中心,它从法律规范、人力投入、管理运营等方面解决了网络信任的多种问题。因此,将二者统一称为“PKI/CA”。PKI/CA 主要组成机构:用户、注册机构和认证中心^[4]。其工作原理如图 1 所示。

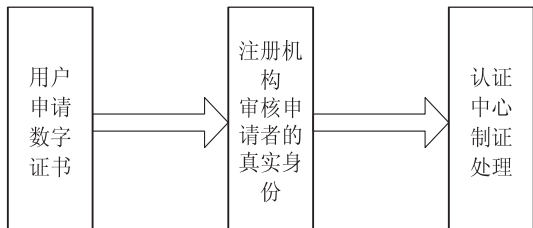


图 1 PKI/CA 的工作原理

如图,注册机构作为用户与认证中心的中间通信,它的主要功能是审核申请者身份的真实性,通过此项审核后,它把用户的信息上传至认证中心,在此进行最后的制证操作。此外,注册机构也会将证书的吊销、更新等提交给认证中心进行处理。由此可见,认证中心可以看作一个可信任的第三方体系,他会为该信任体系中的所有用户发放一张数字证书,以此证明他的身份已经通过鉴定。所以每次交易时,能够方便快速地

判定是否为此信任体系中用户的最有效方法就是:对双方的数字证书进行检查。

这种 PKI/CA 技术以数字证书为核心,能够对网络中传输的信息进行加密和解密、签名和验证,以此确保:除了发送方和接收方外,电子邮件无法被其他人获得,在传输过程中邮件不被更改,通过数字证书,发送方能够确认接收方身份是否真实,对于自己发出的信息,发送方无法抵赖。

PKI/CA 体系加密技术较为成熟,但应用于电子邮件加密时仍然存在一些不足,如:

(1)管理密钥不方便;

(2)进行加解密操作的前提是:需要先交换密钥,此过程繁琐;

(3)一个完整且有效的 CA 系统至少应具有以下部分^[5]:公钥密码证书、历史密钥、黑名单的管理,密钥的备份与恢复,自动更新密钥等。综上,CA 证书获得比较麻烦,这种电子邮件加密技术一直很难普及。

这种传统非对称密钥体系(PKI/CA)加密技术只适用于企业、单位、一些高端用户和高端电子商务中。

2.3 链式加密技术

链式加密技术是一种新颖而又巧妙的邮件加密技术,这种技术将对称密钥算法和非对称密钥算法结合起来,这种加密技术的工作方式是(见图 2):发件人 A 选择一个随机生成的密钥(称之为会话密钥,且每次加密都不同),然后使用对称加密算法(如 IDEA、3DES^[6]等算法)对明文进行第一次加密,再用非对称算法 RSA 进行二次加密。对于收件人 B,他首先用非对称算法 RSA 解出这个会话密钥,然后使用对称加密算法二次解密,最后得到邮件明文。

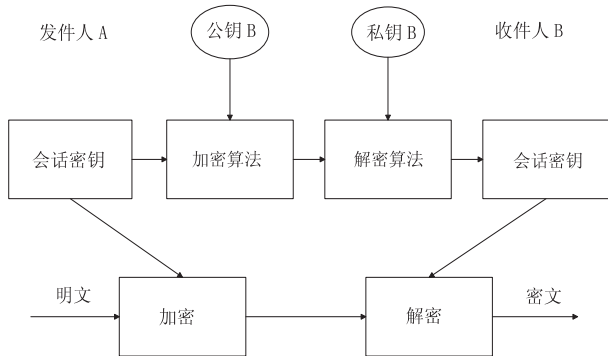


图 2 链式加密技术工作原理

由此可知,以上链式加密技术结合了两种加密算法的优点,它既有对称加密算法的快速性,又有 RSA 算法的认证性和强保密性。另外,在链式加密技术中,用户自己管理密钥,而公钥的交换依赖于信任机制^[7]。因此,用户的电子邮件是绝对安全的。目前著名的电子邮件加密软件 PGP 就是采用这种技术进行加密的^[8]。

2.4 基于身份的密码加密技术

1984 年,以色列著名科学家、RSA 体系的发明者之一 A. Shamir 提出了基于身份密码的思想^[9],大幅度地简化了传统公钥密码系统中密钥管理问题。基于身份的加密(Identity Based Encryption, IBE)是一种新型的公钥加密体制,加密用的公钥不是从公钥证书中获得的,而是直接使用表示用户身份的字符串作为公钥,它的工作原理可通过发送方 A 和接收方 B 之间的具体通信来体现:用户公钥使用发送方 A 自己公开的身份信息(如姓名、身份证号、E-mail 等),而用户私钥是由另外一个可信任的第三方(称之为可信中心)生成。可信中心确认发送者 A 身份准确无误后,将生成的私钥传回给接收方 B, B 再利用此私钥进行解密。这就是经典的基于身份密码加密技术,如图 3 所示。

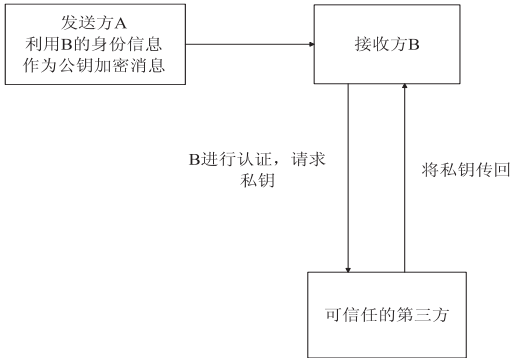


图 3 基于身份加密技术工作原理

由于基于身份加密不需要公钥证书及相关操作,简化了公钥的使用与管理,所以这种加密技术提出后的二十余年中,它就成为了密码学中的研究热点^[10]。作为一种新的公钥密码机制,基于身份加密技术在建设成本、管理效率和计算优化等方面较传统 PKI 有很大提升,被看作是未来构建公钥信任体系的一种有效手段。但是在此体系中,用户的密钥都是被托管在服务器端,所以服务器的安全性以及服务提供者的承诺^[11]对用户信息保密性至关重要。目前典型的基于身份密码的邮件加密产品是赛曼邮件天使系统^[12]。

3 四种邮件加密技术的比较

随着信息技术的发展,邮件加密技术也经历了由简单到复杂、愈加成熟的不断发展过程,综合上述四种邮件加密技术,可得到它们各自的优缺点,见表 1。

由此可见,电子邮件的加密技术日趋成熟,针对不同的系统,结合不同的特点,应该选用其适当的邮件加密技术,以达到最好的效果。

4 结束语

通过以上四种对电子邮件加密技术的分析与研究,将电子邮件加密技术的发展及每种加密技术的原

表 1 电子邮件加密技术比较表

常用邮件加密技术	优点	缺点
对称加密技术	算法公开、计算量小、加密速度快、加密效率高	使用相同密钥、安全性较低、容易泄漏
传统非对称密钥体系(PKI/CA)加密技术	保证身份的真实性和不可抵赖性	密钥管理复杂,CA 证书获得较麻烦
链式加密技术	速度快、安全性高	证书维护、撤销等操作需要的成本较高
基于身份的密码加密技术	不需要任何证书,接收方的公共密钥源自他的身份信息 密钥设有使用期限,因此不需要予以撤销 能够抵御垃圾邮件的攻击	需要一个集中服务器,增大了泄漏的安全风险

理和特点详细呈现出来,文中分析目前常用的四种加密技术各有所长,开发者应该有所取舍,选择合适的加密技术,既提高加密速度,又提高电子邮件的安全性。确保电子邮件系统的正常运行。目前电子邮件系统的安全性仍然会遇到泄密的危险,所以对于其加密的研究将会面临更多的挑战,需要不断地深入探讨,以保证在虚拟的网络世界里,用户拥有绝对安全的隐私权。

参考文献:

[1] 许海玲,吴 潇,李晓东,等. 互联网推荐系统比较研究[J]. 软件学报,2009,20(2):350-362.

[2] 张 琳. 基于 PKI 的电子商务安全研究[J]. 电子科技大学学报,2009,38(Sup):101-103.

[3] Shamir A. How to share a secret[C]//Proc of communications of the ACM. Boston, America:[s. n.],1979.

[4] Paillier P. Public-key cryptosystems based on composite degree residuosity classes [C]//Proc of cryptology - EURO-CRYPT'99. Prague, Czech republic:[s. n.],1999:223-238.

[5] 陈建奇,张玉清,李学农,等. 安全电子邮件的研究与实现[J]. 计算机工程,2002,28(6):121-122.

[6] 李 琦,吴建平,徐明伟,等. 一种前向安全的电子邮件协议[J]. 电子学报,2009,37(10):2302-2308.

[7] 张焕国,王张宣. 密码学引论[M]. 第 2 版. 武汉:武汉大学出版社,2009.

[8] 樊成丰,林 东. 网络信息安全与 PGP 加密[M]. 北京:清华大学出版社,1998.

[9] Shamir A. Identity-based cryptosystems and signature schemes[C]//Advances in cryptology-crypto84. [s. l.]:Springer-Verlag,1984:47-53.

[10] 付晓光,汪秉文,王文顺. 基于电子邮件方式传输数据的软件模块设计[J]. 计算机技术与发展,2007,17(4):235-238.

[11] 向永红,张春霞,张建军. 计算理论研究的核心问题与方向[J]. 计算机与现代化,2000(1):10-15.

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

对电子邮件加密技术的分析与研究

作者：[张瑞丽](#)，[杨坤伟](#)，[李吉亮](#)，[ZHANG Rui-li](#)，[YANG Kun-wei](#)，[LI Ji-liang](#)
作者单位：[陕西师范大学 计算机科学学院, 陕西 西安, 710062](#)
刊名：[计算机技术与发展](#)

ISTIC

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2014(1)

本文链接：http://d.wanfangdata.com.cn/Periodical_wjfz201401040.aspx