PKI技术及其应用的分析

邓晓军
(湖南工业大学 信息工程系,湖南 株洲 412000)

摘 要:主要阐述构建网络安全基础与核心技术——公钥基础设施(PKI,Public Key Infrastructure),它是解决网络交易和通信安全问题的一套完整解决方案。对PKI技术进行了全面的分析和总结,其中包括PKI组成、证书认证机构CA,给出了它的实际应用和发展状况以及未来的发展趋势。讨论了在我国开展PKI应用中存在的一些关键问题,并针对这些问题提出了推广PKI观念、规范PKI建设等相关的解决办法。

关键词:信息安全;公钥基础设施;数字签名;数字证书
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)06-0144-04

Analysis of PKI Technology and Its Application

DENG Xiao-jun
(Department of Information Engineering, Hunan University of Technology, Zhuzhou 412000, China)

Abstract: PKI is the complete solution of network's transaction and information security. It is the basic and main technology to construct network security. It introduces the components of PKI and analyses the actuality of PKI technology. And aiming to this basic and core technology, which is currently used in building secure network, discusses the problems existing in developing PKI in our country. And relevant solutions for example generalizing concept of PKI to these problems have been put forward as well.

Key words: information security; public key infrastructure; digital signature; digital certificate

0 引 言

进入20世纪以来,随着计算机技术和网络技术的飞速发展,Internet/Intranet以及信息技术的广泛普及,社会和经济发展成逐渐依赖于一个错综复杂的信息网络,它改变了人们传统的生活方式、生产方式与管理方式,并对推进国家现代化、推进社会文明的发展,发挥着日益重大的作用,所有这一切正是得益于互联网络的开放性和匿名性的特征。然而,网络本身的开放性和匿名性决定了它在为人们提供快捷与便利的同时,不可避免地存在信息安全隐患。信息安全已成为世界各国所面临的现实问题。目前,网络上主要面临的安全威胁有:

(1)中断:对网络的可用性进行攻击,破坏系统中的硬件、线路及文件系统等,使系统不能正常工作。

(2)窃听:指的是数据在计算机或者其他设备中进行存储、处理、传送等过程中,被别人非法窃取的行为。窃听的方法有很多,如网络窃听是利用数据在网络传递的过程中进行窃听,黑客入侵是利用非法获得的用户权限窃取,电磁辐射是利用电磁辐射信号还原等。

(3)篡改:对完整性进行攻击,篡改系统中的数据内容,修改消息次序、时间。

(4)仿造:破坏真实性,将伪造消息注入系统,假冒合法用户接入系统,重放截获的合法消息实现非法目的,否认消息的接收或发送等[1]。

近几年来我国网络技术已经逐步应用于电子商务、网络银行、网上证券等行业,而这些网络交易活动面临着上述的威胁,对重要信息的传递和控制也非常困难,一旦受到攻击,就很难辨别所收到的信息是否是由某个确定的实体发出的,以及在信息的传递过程中是否曾被非法篡改过。面对以上问题,世界各国纷纷开展了以公开密钥加密技术为基础的公钥基础设施(Public Key Infrastructure,PKI)的研究和应用,同时完善并正确地实施PKI系统是全面解决所有网络交易和通信安全问题的最佳途径。

1 PKI的组成

PKI是一个提供强大开放的数据加密和支持加密服务的典型方法。PKI基础设施采用证书管理公钥,

收稿日期:2007-09-05
基金项目:湖南省教育科研项目(D066106)
作者简介:邓晓军(1974-),男,湖南株洲人,讲师,研究方向为网络与信息安全。

通过第三方的可信任机构——认证中心(Certificate Authority),把用户的公钥和用户的其他标识信息捆绑在一起,在 Internet 网上验证用户的身份。PKI 基础设施把公钥密码和对称密码结合起来,在 Internet 上实现密钥的自动管理,保证网上数据的安全传输。一个有效的 PKI 系统必须是安全的和透明的,用户在获得加密和数字签名服务时,不需要详细地了解 PKI 的内部运作机制[2]。它能提供如下安全服务:

● 身份认证(Authentication):信息的接收者应该能够确认信息的来源,使得交易双方的身份不能被入侵者假冒或伪装;

● 数据的机密性(Confidentiality):确保一个计算机系统中的信息和被传输的信息仅能被授权让读取的各方得到;

● 信息的完整性(Integrity):信息接收者应该能够验证接收到的信息在传送过程中没有被篡改,因此入侵者不可能用虚假消息代替合法消息;

● 不可抵赖性(Non - Repudiation):交易一旦达成,发送者事后不能否认他所发送的消息。

PKI 可以解决绝大多数网络安全问题,并初步形成了一套完整的解决方案。该体系在统一的安全认证标准和规范基础上提供在线身份认证,它是 CA 认证、数字证书、数字签名以及相关安全应用组件模块的集合。作为一种技术体系,从技术上解决网上身份认证、信息完整性和抗抵赖等安全问题,为网络应用提供可靠的安全保障。一个典型的 PKI 系统如图 1 所示,其中包括 PKI 策略、软硬件系统、证书机构 CA、注册机构 RA、证书存储系统和 PKI 应用等。

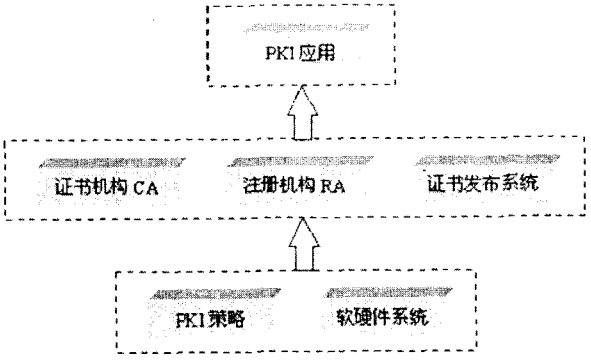

图 1　PKI 系统组成

2　PKI 的应用

2.1　PKI 应用现状

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。当然,作为一种基础设施,PKI 的应用范围非常广泛,并且在不断发展之中,下面给出几个应用实例。

(1)虚拟专用网络(VPN)。

VPN 是一种架构在 PKI 上的专用数据通信网络,利用网络层安全协议(IPSec)和建立在 PKI 上的加密与签名技术来获得机密性保护。基于 PKI 技术的 IPSec 协议现在已经成为架构 VPN 的基础,它可以为路由器之间、防火墙之间或者路由器和防火墙之间提供经过加密和认证的通信。由于 IPSec 是 IP 层上的协议,因此很容易在全世界范围内形成一种规范,具有非常好的通用性,而且 IPSec 本身就支持面向未来的协议—IPv6。总之,IPSec 还是一个发展中的协议,随着成熟的公钥密码技术越来越多地嵌入到 IPSec 中,相信在未来几年内,该协议会在 VPN 世界里扮演越来越重要的角色。

(2)安全电子邮件。

作为 Internet 上最有效的应用,电子邮件凭借其易用、低成本和高效已经成为现代商业中的一种标准信息交换工具。随着 Internet 的持续增长,商业机构或政府机构都开始用电子邮件交换一些秘密的或是有商业价值的信息,这就引出了一些安全方面的问题,包括:消息和附件可以在不为通信双方所知的情况下被读取、篡改或截掉;发信人的身份无法确认。电子邮件的安全需求也是机密、完整、认证和不可否认,而这些都可以利用 PKI 技术来获得。目前发展很快的安全电子邮件协议是 S/MIME (The Secure Multipurpose Internet Mail Extension),这是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

(3)Web 安全。

SSL(Secure Socket Layer,安全套接层)协议是由网景公司研究制定的基于 Web 应用的安全协议。该协议向基于 TCP/IP 的客户/服务器应用程序提供了客户端和服务器的身份鉴别、数据机密性和数据完整性保护。通过在应用程序进行数据交换前交换初始握手信息来实现有关的安全特性,以此实现对应用层透明的安全通信。结合 SSL 协议和数字证书,PKI 技术可以保证 Web 交易多方面的安全需求,使 Web 上的交易和面对面的交易一样安全。

(4)电子商务的应用。

SET(Secure Electronic Transactions)协议是 PKI 技术解决电子商务安全问题的关键,它是由 Visa 和 Master 机构共同制定的一个能保证通过开放网络进行安全电子支付的技术标准。在通信中,利用数字证书可消除匿名带来的风险,利用加密技术可消除开放网络带来的风险,同时保证消息的不可否认性,这样商业交易就可以安全可靠地在网上进行。

2.2 应用前景

近几年随着 PKI 技术应用的不断深入,PKI 技术本身也在不断发展与变化,主要体现在以下几方面:

(1)属性证书。

X.509 v4 证书,它增加了属性证书的概念。与属性证书最为相关的就是授权管理基础设施(PMI,Privilege Management Infrastructure)。PMI 授权技术的核心就是以资源管理为核心,将对资源的访问控制权统一交由授权机构进行管理,即由资源的所有者来进行访问控制管理。

在 PKI 信任技术中,授权证书非常适合于细粒度的、基于角色的访问控制领域[2]。X.509 v4 中引入了公钥证书扩展项,这种证书扩展项可以保存任何类型的附加数据。传统的 X.509 公钥证书为某个人的身份提供不可更改的证据。X.509 v4 能够提供一个人比其身份信息更为重要的权限或者属性信息。具有这样的灵活性就使得通过更改证书的扩展项,能够满足不同应用的需求。

(2)无线 PKI(WPKI)。

随着无线通信技术的广泛应用,无线通信领域的安全问题也引起了广泛的重视。将 PKI 技术直接应用于无线通信领域主要有两个方面的约束:其一是因为无线终端设备的资源有限,即它们的运算能力、存储能力、电池寿命都相对有限;其二是不同的系统之间通信模式不同。为满足这些需求,目前已公布了 WPKI 草案,其内容涉及 WPKI 的运作方式、WPKI 如何与现行的 PKI 服务相结合等。对 WPKI 技术的研究与应用正处于探索之中,它代表了 PKI 技术发展的一个重要趋势[3]。

世界各国为建立安全及可信赖的电子交易环境,普及电子商务的应用,莫不致力于推动与电子签章相关的立法工作。全球电子商务立法,是近几年世界商事立法的重点,电子商务立法核心主要围绕电子签章、电子合同、电子记录的法律效力开始[4]。2005 年 4 月 1 日,《电子签名法》在我国正式实施。据统计,到 2006 年底,获准从事电子认证服务的机构已经有 22 家,遍布全国 17 个省市。这 22 家机构发放的证书共 546 万张、广泛地应用到包括网上税务、电子报关等电子政务领域,网上银行等电子商务领域,还涉及工商、税务、海关、药监等各类体系。2006 年我国数字证书服务市场规模达到 4.5 亿元,较 2005 年增长约 22%[5]。

3 存在的问题

因为 PKI 的应用能跨越多个行业和领域,现在国内许多行业已陆续投入 PKI 建置,目前我国已经成功建设大型的行业性或区域性的 PKI/CA 就有四十多个,这些 PKI/CA 中心广泛用于电子商务和电子政务。但是由于我国信息领域基础薄弱、起步晚,对 PKI 的应用并不熟悉以及 PKI 业务本身操作的复杂性,严重地阻碍了 PKI 的发展和普及,有如下几个方面亟待解决:

(1)PKI 观念有待推广。

随着 Internet/Intranet 的逐渐普及,电子购物、电子支付、网络银行、电子政务等业务走进了人们的视线。虽然目前对于安全的需求日益增长,但是还有许多政府、企业领导或个人并没有意识到网络安全的重要性,同时也不知道 PKI 对于实现网络安全的重要程度。

另一方面 PKI 机制虽然满足了信息安全的基本要求,但其使用或申请手续繁杂,常导致客户或业主为求便利,而宁可牺牲一些安全。目前无论个人或企业,虽然都认同安全的重要性,但对 PKI 的使用经验仍属缺乏,因此提升全民对电子商务和政务,以及电子签名的认知与接受与否,是另一重要的问题。

(2)政府应该规范 PKI 的建设。

我国正热火朝天地进行 PKI 建设。影响最大的行业性 PKI/CA 有:中国金融认证中心(CFCA)、中国电信认证中心(CTCA);影响最大的区域性 PKI/CA 有上海 CA 认证中心和广东 CA 认证中心[5]。这些 CA 中心主要用于电子商务。各级政府也在建设 PKI/CA,主要用于电子政务。

现在主要的问题是国家缺乏统一的规范和管理部门来指导 PKI 的建设问题,导致了许多重复的建设。同时,虽然国内的 PKI 厂商都称他们支持 X.509 证书格式,但由于证书的一些扩展项选择不一样,证书的接口标准不同,所有这些都使得各家的 PKI/CA 基本上处于相互分割的状态,证书之间不能进行互操作,这严重影响了证书的应用,同时也制约了 PKI/CA 的运行规模和效率,在一定程度上影响了人们对 PKI 的使用。就我国而言,从市场的需求及未来发展看,有五、到六个认证中心足矣。即使是在电子商务很发达的美国,也只有两、三个大型的认证中心。现在国内一哄而上建认证中心,完全没有必要。已经有中国电信的 CA(CTCA)、中国人民银行的 CA(CFCA),它们都是利用国外先进经验,采用自主安全技术构建的大型 CA 中心,已经获得"国家信息安全认证",起点都比较高。以后再重点发展一到两个商业性 CA,当时机成熟时,在此基础上再建一个国家级的根 CA,全国的认证问题基本上就解决了。

(3)交互认证问题有待解决。

由于经济全球化的影响,应该以前瞻的目光来发展我国的PKI。由于电子商务多为全球跨国界行为,因此CA与CA间特别是国与国之间CA的交互认证问题亦有待解决,而这其中所涉及的问题除技术层面外,政治与经济利益等因素也是用户或国家考虑的重点。目前国内相关专家学者已考虑三种可行解决方案,即Root CA、Bridge CA及OCSP(Online Certificate Status Protocol) Responder(即证书状态在线查询)。无论未来我国会以何种方案来实施,必须既要考虑建立统一的国家证书管理中心来解决CA交互认证问题,还要尊重并依循市场发展机制,提供统一数据查询平台,供一般使用者在线查询数字证书合法性及有效性,使数字证书的相关业务朝更多元化发展。

4 结束语

据IDC调查,全球PKI市场正在急剧扩大,预计到今年有望达到30亿美元的规模[6]。若针对以上在建制PKI系统中提出的问题采取较好的应对措施,这将会极大促进PKI在我国各行业的应用和普及,推进我国信息化建设。

参考文献:

[1] 李明柱. PKI技术及应用开发指南[EB/OL]. 2002-06-12. www.developerworks.com.

[2] 谷和启. 公钥基础设施PKI技术与应用发展[EB/OL]. 2003-11-10. http://network.ccidnet.com.

[3] 从国际电子商务立法到中国的电子商务政策法律环境[EB/OL]. 2004-07-13. http://www.chinaeclaw.com.

[4] 吴世忠. 规范CA认证中心的建设已成当务之急[N]. 光明日报,2000-07-19(B1).

[5] 卢旭成.《电子签名法》实施两年成绩显著,电子认证服务:在规范中开拓发展[N]. 中国计算机报,2007-05-09(A2).

[6] 余 勇. 标准化推动PKI发展[EB/OL]. 2003-06-27. http://www.ccidnet.com.

(上接第141页)

[3] Susilo W, Safavi-Naini R, Pieprzyk J. RSA based fail-stop signatures schemes[C]//International Workshop on security. Washington, D C, USA: IEEE Computer Society Press, 1999: 161-166.

[4] 马春波,何大可. 门限失败—停止签名[J]. 计算机工程与应用,2004(19):145-146.

[5] 杨 波. 现代密码学[M]. 北京:清华大学出版社,2003:143-181.

[6] 卿斯汉. 安全协议[M]. 北京:清华大学出版社,2005:66-75.

(上接第143页)

又 $e = r^{-1}e' = r^{-1}r_x m' = r^{-1}r_x r m_x m_y = r_x m_x m_y$

由上可知,该签名能通过验证。

(2) 盲性。盲性是盲数字签名的重要特性,匿名意味着签名者不知道需要签名的真实内容。在此方案的签名过程中,签名者B在不知道用户A的盲因子的情况下,只能获得用户A盲化后的信息m',而由m'得到m等价于求解椭圆曲线离散对数问题,所以签名者不可能看到明文消息。

(3) 不可伪造性。任何人要伪造签名(y,e),并通过验证方程$e = r_x m_x m_y \bmod l$的检验,其困难性等价于求解椭圆曲线离散对数问题。

(4) 不可追踪性。假设签名者保留(y,e,m',R'),若签名者想追踪签名,他需要通过盲化消息m'求得有关A的秘密信息,但是由于m'求解m的难度等价于求解椭圆曲线的离散对数问题,所以在签名被接收者泄露后,签名者不能追踪签名。

3 结束语

设计了一种基于椭圆曲线密码体制的盲数字签名及其身份识别方案,具有较高的安全性,并在电子商务、电子投票中具有一定的理论和实用价值。众所周知,目前还没有有效求解椭圆曲线离散对数问题的算法,所以该方案目前是安全的。

参考文献:

[1] Fan C I, Chen W K, Yeh Y S. Randomization enhanced Chaum' blind signature schemes[J]. Comput. Commun, 2000,23:199-203.

[2] Shao Z. Improved user efficient blind signatures[J]. Electronic Letter,2000,36(16):209-219.

[3] Chaum D. Blind Signature System[C]//Advances in Cryptology, CRYPTO'83. NEW YORK: Spring Verlag,1983.

[4] 杨义先,钮心忻. 应用密码学[M]. 北京:北京邮电大学出版社,2005:133-147.

[5] 冯登国. 密码分析学[M]. 北京:清华大学出版社,2000.