校园网络环境下数字签名的研究与设计

刘 涛,潘道远
(安徽工程科技学院 计算机科学与工程系,安徽 芜湖 241000)

摘 要:校园网是社会信息化发展的必然产物,它担当着教学、科研、管理和对外交流等许多角色,因此其安全性非常重要。使用了一种数字签名方案来解决校园网络系统中消息传输的安全性问题,该方案是采用哈希函数 MD5 算法来计算消息摘要,用 RSA 算法实现数字签名,并用 ASP 实现了基于 SQL 的密钥管理和数字签名与验证。

关键词:校园网;数字签名;RSA算法;公钥
中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2007)12-0128-04

Research and Design of Digital Signature Based on Campus Network Environment

LIU Tao, PAN Dao-yuan
(Dept. of Computer Sci. & Techn., Anhui Univ. of Techn. & Sci., Wuhu 241000, China)

Abstract: The campus net is the result of the developing of the social information, which acts many roles like teaching, scientific studies, management and outward exchanges. In this case, its safety becomes one of important research lessons. The design adopts a kind of digital signature to solve the safety problem of message transmit in the campus network system, the strategy uses the algorithm of Hash MD5 to calculate message summary, adopts the algorithm of RSA combined. This issue also expounds the concrete process that realizes of project from the design of algorithm.

Key words: campus network; digital signature; RSA algorithm; public key

0 引 言

随着计算机技术的发展和普及,校园信息网的建设也卓见成效,大家所熟悉的 CIS(Campus Information System)建设就是校园现代化管理的重要手段之一。校园网络作为学校重要的基础设施,担当着学校教学、科研、管理和对外交流等许多角色,校园网安全状况直接影响着学校的教学活动。为了保护数据和资源的安全,校园网必须要求具有高度的可靠性和安全性,因此在校园网络上传输的数据必须具有抗否定性、完整性、安全性以及身份验证机制。数字签名技术这种能保证数据的完整性、机密性、抗否定性的信息安全技术毫无疑问将会在校园网络系统中得到广泛的应用。

在网络上传送的文件是通过数字签名来证明当事人身份与数据真实性和完整性的,要求发送者事后不能否认发送的报文签名;接收者能够核实发送者发送的报文签名;接收者不能伪造发送者的报文签名;接收者不能对发送者的报文进行部分篡改;网络中的某一用户不能冒充另一用户作为发送者或接收者;它可以解决否认、伪造、篡改及冒充等问题[1]。RSA 密码体制由 Shamir、Rivest 和 Adelman 在 1979 年提出,它是第一个也是应用最广的公钥密码体制。经过 20 多年的密码分析和攻击,迄今为止,RSA 被证明仍是安全的。因此,基于 RSA 算法的校园网络环境下的数字签名非常可行。

收稿日期:2007-03-09
基金项目:安徽省自然科学基金资助项目(2005kj065);安徽省高校青年科研资助计划项目(2006jql149)
作者简介:刘 涛(1973-),女,安徽六安人,讲师,硕士,研究方向为软件工程、信息安全等。

1 校园网络面临的安全威胁及其防范措施

影响校园网络安全的因素很多,既有自然因素,也有管理方面因素。

通过多方面的调查与研究,构成对校园网络的威胁主要有[2]:人为失误;网络管理上的漏洞;网络病毒;系统的漏洞;网络窃听;重放攻击;假冒;拒绝服务攻击。

由于网络所带来的诸多不安全因素,使得网络使用者必须采用相应的网络安全技术和安全控制策略来堵塞安全漏洞以保证信息的安全。校园网络安全问题

是一个系统工程,不是单纯的技术问题。因此必须从系统的观点去考虑。针对上面的一些安全问题,总结出了若干对策措施[3]。

通过入侵检测等方式定期对校园网进行漏洞扫描,审计跟踪;在校园网络服务器和各个工作站点上安装相应的防病毒软件,由校园网络安全中心统一控制和管理,实现全网统一防病毒。采用防火墙技术;制订完善的内部管理和审核制度、信息监督制度;在校园网络安全上,采用分层控制方案;划分子网运用 VLAN 技术,将网络按功能划分成若干个子网;建立账号和密码管理机制;采用加密技术。

通过加密技术处理后的信息只能供经过允许的人员,以经过允许的方式使用,能够有效地防止信息在传输中非法泄密。加密技术采用硬件与软件的方式都可以实现,其灵活性较高,应用范围广,下面将对其进行详细的阐述。

2　数字签名

密码系统是一个 5 元组 (E,D,M,K,C),M 是明文集,K 是密钥集,C 是密文集,$E:M\times K\rightarrow C$ 是加密函数集,$D:C\times K\rightarrow M$ 是解密函数集。计算机密码体制的基本思想就是将要保护的信息变成伪装信息,只有合法的接收者才能从中得到真实的信息。密码体制有对称密钥体制和非对称密钥体制之分,文中所重点讲述的 RSA 公钥体制便为非对称密钥体制,也叫做公开密钥体系。

ISO7498－2 标准对数字签名做了如下解释:“附加在数据单元上的一些数据,或是对数据单元所作的密码变换,这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性,并保护数据,防止被人(例如接收者)进行伪造”。数字签名在美国电子签名标准(DSS,FIPS186－2)中定义为:“利用一套规则和一个参数对数据计算所得的结果,用此结果能够确认签名者的身份和数据的完整性”。数字签名是目前电子商务、电子政务中应用最普遍、技术最成熟的、可操作性最强的一种电子签名方法。

数字签名的方法有多种,这些方法可分为两类:基于对称密码的数字签名和基于公钥的数字签名。

2.1　基于对称密码的数字签名

在对称密码体制中,只有收发双方掌握密钥,所以它可以有效地实现信息的保密性,但是不能杜绝接收方的伪造的发送方的否认行为,即不具备签名功能,若要利用对称密钥实现数字签名,必须有可信任第 3 方的支持,签名由第 3 方转发。该方法的缺点是增加了网络和第 3 方的负担,另外还存在着如何分发和存储用户共享密钥的问题[4]。

2.2　基于公钥的数字签名

自从公钥思想诞生以来,公钥密码体制得到广泛的重视,并在数字签名方面得到很好的应用。基于公钥的数字签名,需有权威认证机构(CA)的支持,CA 主要是对公钥进行管理并起到仲裁的作用。用户 A 若想发送签名给用户 B,则 A 用私钥 K_A 利用签名函数 H 对信息 M 进行签名,并将 M 和签名文发送至 B,B 从 CA 那里获得 A 的公钥 Q_A 对 A 发来的签名进行验证。目前典型的用于数字签名的公钥算法为 RSA,DSS 等[4]。

3　算法选择

在后面的方案设计中采用了 MD5 算法和 RSA 算法,这都是经过同类算法的比较以及权衡校园网的一些特点后选择的。

3.1　MD5 算法

MD5 的全称是 Message－Digest Algorithm 5(信息－摘要算法),于 20 世纪 90 年代初由 MIT Laboratory for Computer Science 和 RSA Data Security Inc 的 Ronald L. Rivest 开发出来,经 MD2、MD3 和 MD4 发展而来。MD5 算法简要的叙述为:MD5 以 512 位分组来处理输入的信息,且每一分组又被划分为 16 个 32 位子分组,经过了一系列的处理后,算法的输出由四个 32 位分组组成,将这四个 32 位分组级联后将生成一个 128 位散列值[5]。

MD5 的典型应用是对一段信息产生信息摘要,以防止被篡改。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,产生一个唯一的 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,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。如果有一个第三方的认证机构,用 MD5 可以防止文件作者的“抵赖”,从而用于对消息的数字签名。

3.2　RSA 算法

RSA 算法概述如下[6]:找两素数 p 和 q,令 $n=p\times q$,令 $f(n)=(p-1)(q-1)$,取任何一个数 e,要求满足 $e<n$ 并且 e 与 $f(n)$ 互素,取 $ed \bmod f(n)=1$。这样最终得到三个数:e,n,d。设消息为数 $M(M<n)$

设　$c=M^e \bmod n$

就得到了加密后的消息 c;

设　$m=c^d \bmod n$

则 $m=M$,从而完成对 c 的解密。

在对称加密中：

(d,n) 两个数构成公钥，对外公布；

(e,n) 两个数构成私钥，e 由用户自己保存。

给别人发送的消息使用私钥 e 加密，只要别人能用公钥 d 解开就证明消息是由你发送的，构成了签名机制。别人给你发送信息时使用 d 加密，这样只有拥有 e 的你能够对其解密。

4 校园网络环境下数字签名的设计与分析

4.1 方案的设计

系统流程设计，本系统流程方案采用验证码技术判断登陆信息的有效性，用用户 ID、口令等一些用户信息验证用户的真实性，同时整个系统基于 B/S 模式。其具体过程如图1所示。

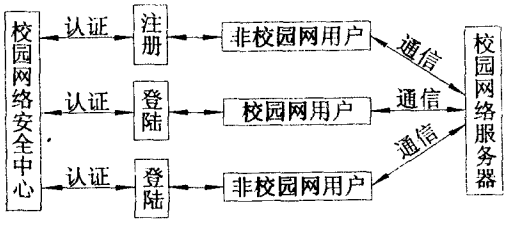

图1 校园网络认证与通信

1) 非校园网用户没有注册的首先向校园网络安全中心申请。如果是校园网用户，由校园网络服务器管理员直接将信息写入服务器，然后转到4)。

2) 校园网络安全中心收到申请后，进行身份认证。

3) 身份认证通过后，由校园网络安全中心将信息直接传递给校园网络服务器。

4) 由校园网络服务器随机产生用户的公钥与私钥，其中公钥存储在服务器中，私钥由用户本人保管。

5) 校园网的所有用户相互通信都通过服务器进行转发。

数字签名设计，本方案采用 MD5 算法计算消息摘要，用 RSA 算法对消息进行加密、解密、签名和验证等功能。具体过程如下：

(1) 发送方 Alice 将发送消息用 MD5 算法进行编码，产生一段固定长度的消息摘要；

(2) 发送方 Alice 用自己的私钥对消息摘要加密，形成数字签名，附加在消息的后面；

(3) 发送方 Alice 用 Bob 的公钥对带有数字签名的消息进行加密，传送给校园网络服务器；

(4) 接收方 Bob 登录校园网络服务器收到加密后的消息，用自己的私钥对其解密，得到数字签名和消息；

(5) 接收方 Bob 用发送方 Alice 的公钥对数字签名解密，得到消息摘要；同时对消息用 MD5 算法编码，产生另一个消息摘要；

(6) 接收方 Bob 将两摘要进行比较，若一致，说明消息是真实的，存储该消息；否则丢弃该消息。

4.2 方案的分析

本方案在加密和数字签名上的算法和相关技术等都是经过比较后选择的，并结合了现有校园网络系统的实际情况，充分证实方案所具有的优越性和可行性。基于 B/S 模式，将公钥密码 RSA 算法的快速、低成本和哈希算法 MD5 的安全性完美地结合在一起。较好地满足了校园网络系统对信息安全传输的要求。校园网系统存在的安全问题主要有：网络侦听；截取/重放；暴力攻击。本方案采用的验证码技术能够很好地解决截取/重放和暴力攻击的安全问题，采用的公钥密码 RSA 算法能够解决网络侦听和数字签名等问题。

5 基于 RSA 算法数字签名的实现

RSA 公钥体制被广泛地应用于数字签名方案之中，其实现过程分为消息摘要、随机大数的产生、素数的产生、密钥的生成和签名、认证等几个步骤。

5.1 求模 n 和欧拉函数 $f(n)$

从前面的理论分析，可以看出要使 RSA 算法具有签名和认证功能，必须先寻找一个大数 n 并求欧拉函数 $f(n)$，其过程为：

(1) 求素数 p,q；

(2) $n = p * q$；

(3) $f(n) = (p-1)(q-1)$。

n 是由两个大素数相乘得到的，因此，大素数的生成是求得 n 的关键。产生素数的一般方法可以分为两类，即概率性素数产生方法和确定性素数产生方法。概率性素数产生方法产生的数仅仅是伪素数。其缺点在于，尽管其产生合数的可能性很小，但是这种可能性仍然存在。其优点是产生的伪素数没有规律性，而且产生的速度也比较快。确定性素数产生方法产生的数必然是素数。然而其产生的素数却带有一定的限制。假若算法设计不佳，便容易构造出带有规律性的素数，使密码分析者能够分析出素数的变化，进而可以猜到该系统中使用的素数。

5.2 密钥对生成

RSA 数字签名的主要工作为大素数的生成、最大公因子 gcd、模 n 求逆 $a^{-1}\bmod n$ 和模 n 的大数幂乘 $x^y \bmod n$ 的算法，最终产生密钥对。上一节，已经讨论了大素数的生成算法，这里主要讨论最大公因子 gcd、求逆 $a^{-1}\bmod n$ 和大数幂乘 $x^y \bmod n$ 的算法。其中最大公因子 gcd 用 Euclid 算法求解；求逆 $a^{-1}\bmod n$ 用扩展

Euclid 算法解决。密钥对生成的过程如下:

(1) 任取一整数 e,满足 $e < f(n)$,并满足 $\gcd(e, f(n)) = 1$;

(2) 求 d,满足 $ed \bmod f(n) = 1$;(e,d) 即为密钥对。

图 2 是利用该算法编写程序,自动生成密钥对的界面图。

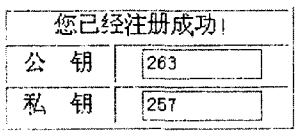

图 2　生成的公钥和私钥

5.3　RSA 算法签名与验证

加密密文过程,为了使用 RSA 加密消息 M(其中 $1 \leqslant M \leqslant N-1$),必须进行下列计算:$c = M^e \pmod n$,其中 c 是密文,然后发送 c。解密密文过程,为了使用 RSA 解密密文 c,必须进行下列计算:$c^d \pmod n = M$,其中 M 是你的原始明文。如果用两对密钥对进行消息的加密与解密,RSA 算法将具有签名与认证的功能[7]。图 3 是 RSA 算法签名与认证的流程图。

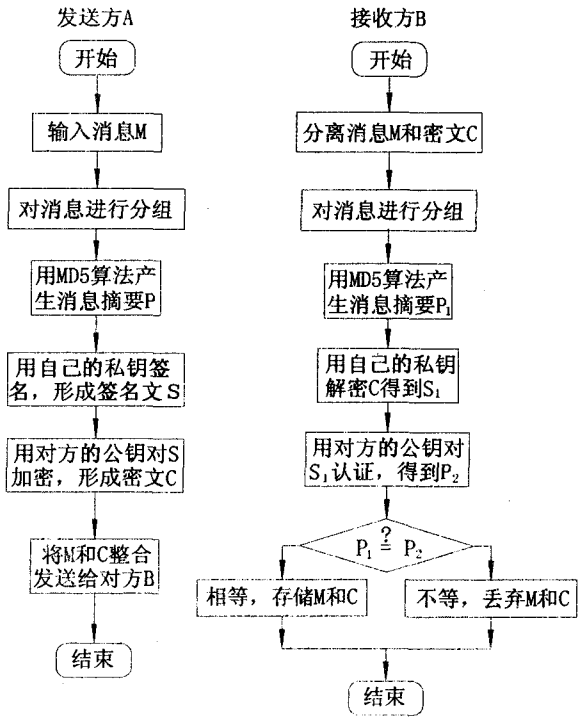

图 3　RSA 算法签名与认证流程图

利用 ASP 编写了一个小型模拟程序对方案进行了验证。过程如下:用户 yanxin 和 biqiong 填写其基本信息进行注册,然后分别进入系统,分别申请公钥与私钥,yanxin 的公钥为 125,私钥为 293。biqiong 的公钥为 221,私钥为 149。其中公钥存入校园网络中心的服务器中,私钥由用户保存。用户 biqiong 在登陆系统后,给用户 yanxin 发送信息,在 to:后面输入接收信息的 id,在私钥后面的文本框中输入自己的私钥 149。并且在信息文本框中输入“Research and Design of Digital Signatures Based on the Campus Network Environment”。然后单击发送按钮(如图 4 所示)。

用户 yanxin 登陆校园网,并且进入自己的邮件箱,可以看到自己的信箱里面里已经有 1 封邮件。然后在私钥框中输入自己的私钥 293,单击查看自己的信箱按钮(如图 5 所示)。

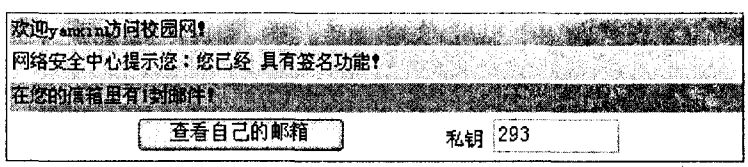

图 5　接收信息界面图

输入 biqiong 的公钥 221,然后系统反馈邮箱里面的内容“Research and Design of Digital Signatures Based on the Campus Network Environment”。与用户 biqiong 发给用户 yanxin 的信息是一样的,并且该条信息是由用户 biqiong 发送的事实是不可否认的。如图 6 所示。

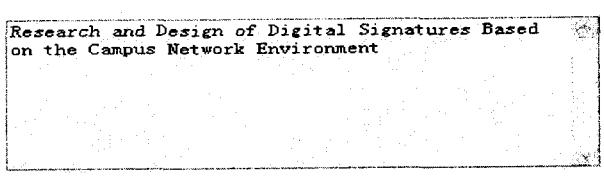

图 6　查看邮箱信息图

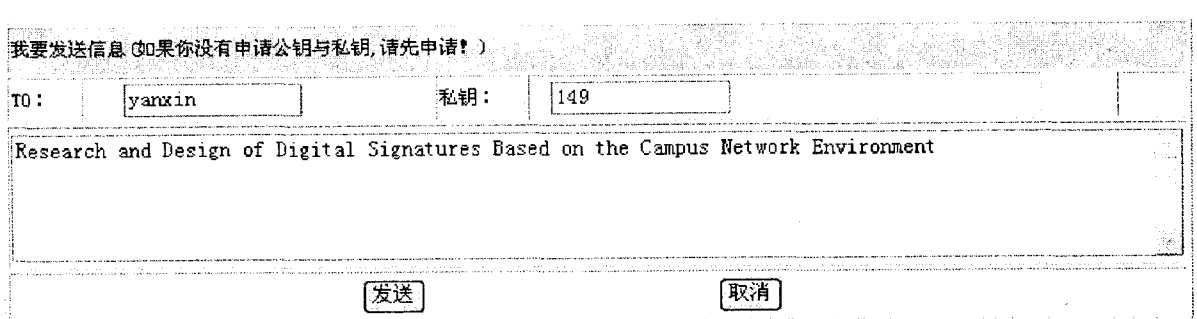

图 4　发送信息界面图

(下转第 135 页)

于该签密方案是公开可验证的。

定理 5　上述签密算法满足前向安全性。

证明:因为任何人虽然均可截获在公开信道上传输的签密(c,R,s),但由于 r 是隐藏在 $R = rG$ 中,这样即使 x_A 丢失,他也不会从 $s = x(r + x_A)^{-1} \bmod q$ 中得到 x,这样只能从 $k_2 = H(x_B k_1)$ 中计算 k_2,这是 ECDLP 问题。因此敌手不能计算加密密钥 k_2。

4　结束语

当签密方案采用小的安全参数时(公共模数为 512 位),与常规的先签名后加密的方法比较,签密的计算代价降低为 58%,消息扩展率为 70%;当采用长的安全参数时(公共模数为 1536 位),签密的计算代价降低为 50%,消息扩展率为 91%,签密的节省代价正比于安全参数的长度,当取较大安全参数时安全性能更佳[8]。

由于签密方案仅需执行一步操作就能实现签名与加密的功能,因而能高效地实现安全、认证的信息传输。文中提出的新的基于椭圆曲线的签密方案,具有机密性、不可伪造性、不可否认性,而且具有前向安全性和公开可验证性等安全特征,在效率上较传统的分两步实现的方法有显著提高,因而在现实环境中,将具有良好的应用前景,特别适用于移动通信的应用场合,以实现移动通信中收发双方相互的认证,而公平第 3 方,即仲裁者可以仲裁发送方和接收方通信中发生的争议。下一步的研究将是如何去设计更高效的签密方案,以进一步提高其应用前景和应用价值。

参考文献:

[1] 王继林.公钥体制下的匿名问题研究[D].西安:西安电子科技大学,2003.

[2] Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption)[C]//in Advances in Cryptology - Crypto' 97. Lecture Notes in Computer Science 1294. Berlin: Springer,1997.

[3] Jung H, Lee D, Lim J, et al. Signcryption Scheme with Forward Security [C]//Proceedings of WISA 2001. [s. l.]: Springer - Verlag,2001.

[4] 李艳平,谭示崇,王育平.一个公开可验证和前向安全的签密方案[J].计算机应用研究,2006(9):98 - 99.

[5] 李新明,李子臣.改进的认证密钥交换协议[J].河南科技大学学报:自然科学版,2003,24(3):58 - 59.

[6] 张　雁,林　英,郝　林.椭圆曲线公钥密码体制的研究热点综述[J].计算机工程,2004,30(3):127 - 129.

[7] 卢开澄.计算机密码学——计算机网络中的数据保密与安全[M].北京:清华大学出版社,2003:282 - 297.

[8] Zheng Y. Digital signcryption and its application in the efficient public solutions[C]//Proceeding of Information Security Workshop(ISW' 97). Berlin: Springer Verlag, 1997: 291 - 312.

(上接第 131 页)

若非法用户盗取了用户 yanxin 的口令和密码,而不知道其私钥,在私钥框中随机输入私钥,将不能看到其消息。

在实际系统中应将私钥设置为不可见的,或者以通常的若干个'*'方式显示。

6　结束语

本方案在加密和数字签名上的算法和相关技术等都是经过比较后选择的,并结合了现有校园网络安全的实际情况,充分证实方案所具有的优越性和可行性。在当今还没有一个较 RSA 密码系统更为优秀的密码系统出现之前,可以有效地改进 RSA 加密算法的速度也是解决当今密码学主要的一个研究方向。

目前大学校园无纸化办公已成为一种趋势,无纸化办公能否顺利地进行,已经引起人们的高度重视。将文中所采用的方案与无纸化办公实现无缝连接还有许多工作要做。

参考文献:

[1] 贺　刚. 数字签名在校园办公网上的实现[J].湖北民族学院学报:自然科学版,2004,22(2):69 - 71.

[2] 周　芳,宫晓曼,腾荣华.对校园网络安全的研究[J].江西科技师范学院学报,2004(5):90 - 92.

[3] 程　线, 戴国梁. 论校园网系统建设安全性及相应策略[J]. 湖南广播电视大学学报,2004(2):24 - 26.

[4] 刘　涛. 基于校园网的成绩 MIS 数字签名的研究与设计[J]. 微机发展,2005,15(11):24 - 26.

[5] Stallings W. 密码编码学与网络安全——原理与实践[M]. 第 3 版. 刘玉珍,王国娜,傅建明等译. 北京:电子工业出版社,2004.

[6] Bishop M. 计算机安全学——安全的艺术与科学[M]. 王立斌,黄　征等译. 北京:电子工业出版社,2004.

[7] 贾俊敏,王纪卿,孔英会,等.电子交易系统中文本安全传输方案研究[J].电力系统通信,2005,26:33 - 35.