第 34 卷 第 11 期 计 算 机 工 程 2008 年 6 月
Vol.34 No.11 Computer Engineering June 2008
·安全技术· 文章编号：1000—3428(2008)11—0174—03 文献标识码：A 中图分类号：TP309.7

一种改进的 PGP 安全电子邮件系统

陈 静[1]，徐 洁[2]，俸志刚[2]
(1. 电子科技大学软件学院，成都 610054；2. 电子科技大学计算机学院，成都 610054)

摘 要：USB安全锁是网络身份认证系统中常用的信息载体，具有较高的可靠性。该文引入N分法密钥概念，结合USB安全锁的认证协议，提出一种改进的PGP电子邮件系统。在安全通信时，利用USB安全锁进行身份认证和密钥管理，无须可信第三方的介入。实验结果证明，该系统可以有效地抵抗重放攻击和中间人攻击。

关键词：加密；USB 安全锁；身份认证

Improved PGP Secure E-mail System

CHEN Jing[1], XU Jie[2], FENG Zhi-gang[2]
(1. College of Software, University of Electronic Science and Technology of China, Chengdu 610054;
2. College of Computer, University of Electronic Science and Technology of China, Chengdu 610054)

【Abstract】 USB device can be used as a USB security key. When it is used as an identity token in an network Identity(ID) authentication system, adopting the correspondence of the USB security key is more safe than having no adoptive correspondence. By introducing the concept of N-dimensional security key and combining a two-way USB security key authentication protocol, this paper proposes an improved PGP e-mail system. Making use of the USB security key to carry on an identity attestation and manage with airtight key while carrying out safety correspondence, this system does not need the help of trusted third party. Experimental result shows that the system resists man-in-the-middle attack and interleaving attack.

【Key words】 encryption; USB security key; Identity(ID) authentication

1 概述

作为目前流行的一种加密软件，PGP将RSA公匙算法的可靠性和传统加密算法的高速度有效地结合，在防止邮件的非法篡改方面性能优越。PGP具有如下优点：对邮件进行保密以防止非授权者阅读；对用户的邮件进行数字签名，使收信人可以确信发信人的身份；让用户可以安全地进行通信，不需要采取任何保密措施来传递密钥。PGP采用了混合加密算法的加密体系，包含 4 个密码算法单元：对称加密算法(IDEA)，非对称加密算法(RSA)，单向散列算法(杂凑函数)，随机数产生器(从用户击键频率产生伪随机数序列的种子)[1]。每种算法都是PGP不可分割的组成部分，PGP集中了几种加密算法的优点。但是PGP也有固有的缺点。通信双方的密钥管理和身份认证是建立在信任度模型的基础上的，每个PGP用户都可以给他认为是真实的公开密钥签发证书，并且可以拥有多个证明机构颁发的证书。然而，这种信任体系的完备性和权威性存在较大隐患，同时在密钥废除时也不可能及时通知到通信双方。在针对外来攻击如重放攻击时，即使在改进邮件加密算法中，PGP也不能很好地保护通信者的安全。如何克服和避免这些安全隐患也就成为了亟待解决的问题。一些学者借用可信中介CA进行密钥安全管理和双方认证，但实际上又增加了中介认证机构CA(无论可信度多高)泄密的隐患。网络通信安全设计应该是建立在不可信任模型的基础上，最安全的通信要求双方互通而无须第三方的认证和密钥管理。为此，笔者提出一种新的密钥认证和管理方法。

2 PGP 的算法原理说明及安全性

PGP 算法是一个杂凑算法，主要由公开密钥算法(RSA)、常规加密算法(IDEA)、散列算法(MD5)组成。

2.1 RSA 算法的原理及其安全性

RSA 算法是在 1978 年首次提出，其既可用于加密又可用于签名的公开密钥算法。它的保密性是基于一个数学假设：对一个很大的合数进行质因数分解是不可能的。RSA 用到的是两个非常大的质数的乘积，用目前的计算机水平是无法分解的。这 2 个很大的质数：一个公开给世界(公匙)；一个不告诉任何人(私匙)。这 2 个密匙是互补的，就是说用公匙加密的密文可以用私匙解密，反过来也一样。

RSA 的安全性依赖于大数分解的难度。目前还没有一种可以便捷地产生一个大质数的算法。因此，PGP 实际采用的方法是产生一个大奇数，对其做费马测试然后测试它的质数性。质数的个数是无穷的，甚至它的分布密度也超出一般人的想象，数论给出的结论表明，n 以内的质数的个数趋近于 $n/\ln n$。但是随着计算机性能的提高和数论的发展，人们也许会找到一种以多项式方式增长的分解算法，虽然目前这种漏洞可以通过增加 RSA 钥匙长度的方法来暂时弥补，但是钥匙长度的倍增影响了加密的效率和可应用的范围。

2.2 IDEA 算法的原理及其安全性

IDEA 是一个迭代分组密码，分组长度为 64 bit，密钥长度为 128 bit。在 IDEA 密码中使用了 3 种不同的运算：逐比特“异或”运算；模 2 加运算；模 2+1 乘运算(0 与 2 对应)。

作者简介：陈 静(1976－)，男，硕士研究生，主研方向：网络安全，嵌入式软件开发；徐 洁，副教授；俸志刚，讲师
收稿日期：2007-08-25 **E-mail：**cjywcy@163.com

IDEA 算法是由 8 圈迭代和一个输出变换组成的。它将 64 bit 的数据分成 4 个 16 bit 子块，令这 4 个子块作 8 圈迭代。每圈迭代都是 4 个子块彼此间以及 16 bit 的子密钥进行异或，MOD2 加运算，MOD2+1 乘运算。任何一轮迭代第 3 子块和第 4 子块互换。该算法所需要的“混淆”可通过连续使用 3 个“不相容”的群运算，在 2 个 16 bit 子块中来获得，该算法使用的 MA-(乘加)结构可提供必要的“扩散”。已证明 IDEA 算法在其 8 圈迭代的第 4 圈之后便不受差分密码分析的影响了。假定穷举法攻击有效的话，那么即使设计一种每秒可以试验 10 亿个密钥的专用芯片，并将 10 亿片这样的芯片用于此项工作，仍需 1 013 年才能解决该问题。由此看出，idea 加解密算法是比较可靠的。

2.3 杂凑函数算法及其安全性

杂凑函数算法采用单向哈希函数算法，将任意长度的输入报文，经过计算得出固定位的输出，称为报文摘要。所谓单向是指该算法是不可逆的，找出具有同一报文摘要的两个不同报文是很困难的；找出具有同一给定报文摘要的两个不同的报文更为困难。由于哈希算法的单向性和严密性，接收方可确保没有其他人能够生成与收到的报文摘要相同的新消息或原始报文的签名。PGP 采用 MD5 算法和 SHA(Secure Hash Algorithm)算法。它接收到一段明文，以 2 bit 数据块为单位，以不可逆的方式转换成 160 bit 的消息摘要(通常比明文更短)，将一串输入码(预映射或信息)转化为长度较短和位数固定的输出序列，即散列值(信息摘要或信息认证代码)。但是任何一种杂凑函数都会产生一定概率的类似散列值，如果攻击者一旦发现规律，就有可能利用这些缺陷(如尝试利用完全不同的文件或数据生成同一个类似散列值)展开攻击。

3 基于 PGP 系统中 USB 安全锁的设计

3.1 USB 安全锁设计及密钥管理功能

在PGP系统中，USB取代网络专门认证中心(CA)对通信双方进行认证。它的实现方法由预处理、加密和解密 3 个部分组成[2]。在预处理部分，根据要实现的功能(加密和身份认证)确定使用的算法(IDEA)和基于“N分法”产生的随机数及随机密钥。在加密部分，对明文分组并将其编码，对编码后的信息进行和随机数合并，然后将密文传送给对方。在解密部分，对密文进行拆分，根据随机数得到密钥，再对密文分组解密并恢复出明文。USB相关软件设计见图 1。

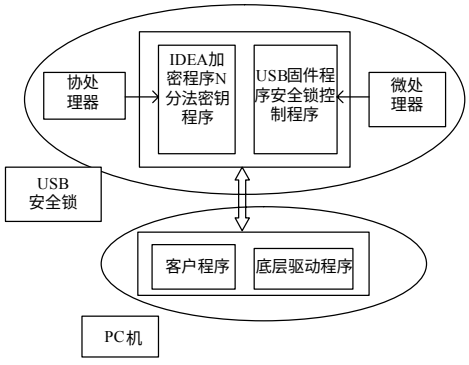

图 1 USB 相关软件设计

在传统 PGP 设计中，IDEA 算法加密的随机密钥是在和邮件加密后一起传输给对方，一旦对方私钥泄漏，IDEA 的密钥也将失去安全性。笔者把产生 IDEA 的随机密钥及算法加密的完成都放在 USB 中实现，同时 IDEA 随机密钥的产生是基于“N 分法”。这样即使在通信过程中，私钥出现泄漏或破解，如果没有接收方的 USB 安全锁，密文还是比较难以破解，因为就现在计算机速度和算法而言，IDEA 还是非常安全的。同时“N 分法”使通信双方不需要密钥交换，因此，基本上避免了因传递而泄漏了密钥的可能性，通信双方的 USB 安全锁自动为通信双方生成了一系列对原文进行加、解密的随机密钥，这使得 USB 安全锁成为 PGP 中最简单易行并且安全的密钥管理办法。

3.2 基于 RSA 的 USB 安全锁认证协议

在基于 RSA 安全通信模型中，考虑到只有合法的 USB 安全锁用户才可以利用此 USB 安全锁进行安全通信，因此，在安全通信之前要对双方的 USB 安全锁及其通信双方的公钥的可信度进行认证，只有证明双方身份及公钥的可信，用户才能使用 USB 安全锁进行安全信息通信。

结合 RSA 的身份认证协议原理、USB 安全锁本身具有的特点，USB 认证模型见图 2。

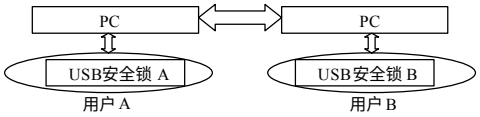

图 2 USB 身份认证

利用 USB 安全锁进行身份和公钥认证过程的如下：

(1)用户 A 插入 USB 安全锁 A 到 PC 的 USB 接口上，并输入自己的用户名 *PN* 和密码 *PS*。

(2)USB 安全锁 A 产生随机数 *R*1，并取得 *T*1(当前时间)和 *T*2(有效时间)，并将以上数据和自身的 *KeyID* 以及 *PN*，*PS* 一起组成明文 *Ma*。

(3)USB 安全锁 A 产生随机数 *R*2 并对 USB 盘里的固定密钥 *UP* 进行“*N*(*n*＝*R*2)分法”产生新的随机密钥 *VUP*。

(4)用户 A 将 *Ma* 使用 VUP 密钥进行 idea 算法加密，其结果和 *R*2 合并成密文 *Ca*，然后使用用户 B 公钥 *Rb*(可以从网站或其他途径获得)对 *Ca* 进行公钥算法，加密成 *Cm* 发往用户 B，如下：

$$Ca\equiv((Ma)^{IDEA}(VUP))\,\|\,R1;\ Cm\equiv Ca^{RSA}Rb$$

(5)用户 B 使用自己的私钥解开加密信 *Cm*，并将其分解为密文和随机数 *R*2。

(6)USB 安全锁 B 接到用户 B 的 USB 接口上，并输入用户 B 的 *PN* 和密码，USB 安全锁 B 上的固定密钥和接收到的随机数 *R*2 利用盘里固定密钥 *UP* 和“N 分法”产生 IDEA 密码 *VUP* 并解开对方的明文 *Ma* 得到随机数 *R*1。

(7)USB 安全锁 B 产生随机数 *R*3 和新的随机密钥 *OVUP*。

(8)用户 B 将 *R*1 和 USB 安全锁的 *KeyID*、*T*3(获取时间)、*PN*(B 的用户名)组成明文并使用 OVUP 密钥进行 idea 算法加密成密文 *Mb*，其结果和 *R*3 合并成密文 *Oca*，将 *Oca* 使用 A 方公钥 *Ra*(也是可以从网站或服务器上获得)进行 RSA 加密成 *Ocm*，并发往 A 方通信 PC 机。

(9)用户 A 用私钥解开 *Ocm* 密文获得随机数 *R*3，并利用 *UP* 和“N 分法”获得随机密钥 *OVUP*，然后进行 IDEA 解密获得明文 *Mb* 及随机数 *R*1，比较获得的 *R*1 和发送的 *R*1，若相同则表示双方的公钥得到认证，并确认对方安全锁的身份和双方获得了安全通信的权限。

(10)用户 A 在有效时间 *T*2 内，没有收到用户 B 的反馈信息，重复(1)，*M*(有效门限)次均未收到用户 B 的消息，认为所得到用户 B 公钥为假或 B 方收件人不在，安全认证过程

终止。

(11)结束。

4　改进的 PGP 电子邮件系统的模型

目前，PGP在网络上的资源是免费的，但是算法程序是相对独立的。PGP的实现依赖于各种邮件客户机。所有的邮件传递都是透明的，不需要用户直接干预，为此，笔者设计了USB安全锁，并依照PGP的原理模型自行实现一组安全加密过程。假定通信双方的公钥和USB身份都得到认证。该通信过程模型把加解密算法如IDEA的密钥及其实现放在USB中去完成，和RSA在PC机上加密分离，所以，一旦当RSA的私钥泄密或者被其他方调换，如果没有USB安全锁，信件内容还是无法取得，IDEA仍是目前最可靠的加解密算法。同时IDEA的随机密钥是由USB的固定密钥和N分法发生器所产生，如果想破解USB的固定密钥，就必须截获连续的$K(K\geq 64)$个报文，并将其全部破译。其中有一个未截获或未破译，都无法破译该密钥。由于N分密钥法可以确保黑客无法连续破译K个报文，使通信系统具有极高的不可破译性，能够抵挡邮件的重放攻击[3]。安全通信过程设计见图 3、图 4。

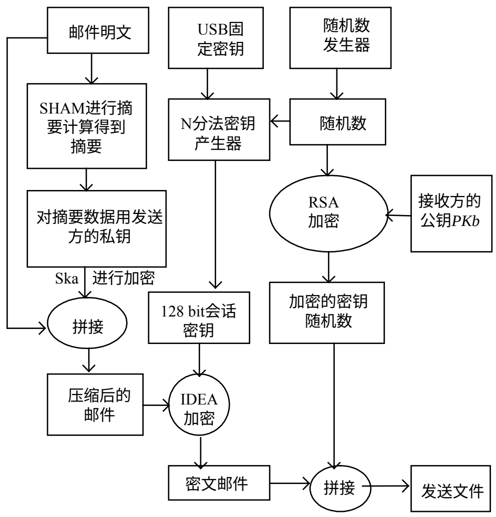

图 3　发送端处理过程

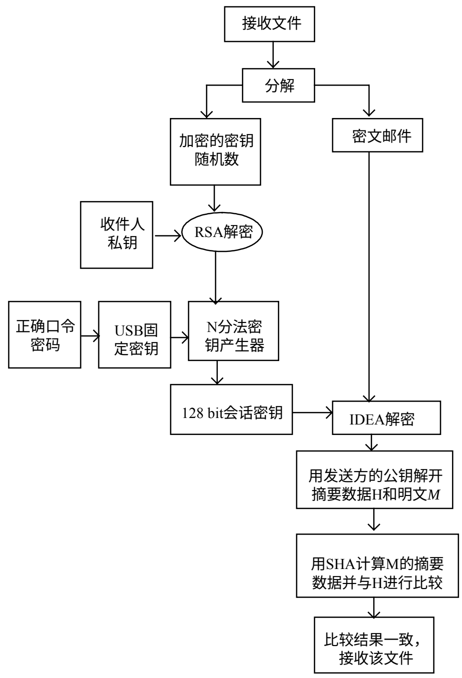

图 4　接收端处理过程

5　结束语

公钥的认证和身份管理是 PGP 系统设计的难点。本文的模型建立在不可信任模型上。USB 的普及使直接通信成为可能，利用独创的 USB 安全锁就可以确定对方公钥的真伪性和通信对方的身份，在 RSA 的公钥加密基础上增加了一层可信度，“ N 分法 ” 对 IDEA 的密钥进行了良好的管理。密钥和算法分开存储的 PGP 系统，实现了真正意义上的安全通信。

参考文献

[1] Networks Associates Technology Inc.. PGP Windows User’s Guide[Z]. 2002.

[2] USB Implement Forum. USB Implement Forum[Z]. 1996.

[3] 李晓波. N 分密钥系统在湖南长沙问世[EB/OL]. (1999-10-01). http://www.3nettel.com/tsxz/mm3.htm.

~~~~~~

（上接第 167 页）

优于单个神经网络分类器的性能。但是，使用不同集成方法其检测性能是不同的。另外，使用不同的聚类技术及不同的融合方法，检测率与误报率是不同的，其中使用 Hier_max 方法获得了较好的性能，可训练的融合方法要比固定的融合方法更能提高检测性能。

由表 3 可以知道，使用 DBNNE, Bagging, Adaboost 集成方法的性能是类似的，这充分说明集成方法 DBNNE 在较大的数据集上与 Bagging 和 Adaboost 相比，性能优越。

参考文献

[1] Kuncheva L I, Whitaker C. Measures of Diversity in Classifier Ensembles[J]. Machine Learning, 2003, 51(2): 181-207.

[2] Aksela M, Laaksonen J. Using Diversity of Errors for Selecting Members of a Committee Classifier[J]. Pattern Recognition, 2006, 39(4): 608-623.

[3] 李　凯, 黄厚宽. 一种提高神经网络集成差异性的学习方法[J]. 电子学报, 2005, 33(8): 1387-1390.

[4] Giacinto G, Roli F, Didaci L. Fusion of Multiple Classifiers for Intrusion Detection in Computer Networks[J]. Pattern Recognition Letters, 2003, 24(12): 1795-1803.

[5] 李　凯, 李昆仑, 崔丽娟. 模型聚类及在集成学习中的应用研究[J]. 计算机研究与发展, 2007, 44(增刊): 203-207.
~~~~~~