基于IDEA算法的存贮加密系统

赵全习， 宋长平， 刘 红
(空军工程大学 导弹学院，陕西 三原 713800)

摘 要:分析了计算机系统存贮信息的内部漏洞和外部威胁,针对存贮数据的范围和特点,结合分组密码的杰出代表IDEA设计了一个存贮加密系统,分析表明,此系统具有强大的安全性、可供选择的密钥管理、良好的实时性和可易实现性。

关键词: 信息安全;IDEA;RSA;数据加密
中图分类号:TP30 **文献标识码**:A **文章编号**:1009-3516(2003)06-0071-03

1 信息存贮的安全性

随着全球信息高速公路建设的兴起和通信的网络化、个人化、智能化、宽带化进程的不断加快,用户对信息的安全存贮,安全处理和安全传输的需求日益迫切。特别地,伴随着Internet的开通，以及个人通信、多媒体通信、办公自动化、电子邮件、电子自动转帐支付系统、自动零售业务网的建立与实现,信息的安全保护问题就更加显著,信息安全是信息的备战,是信息有效防御的结果。加密,则是信息安全的关键和核心[1]。信息安全虽然包括了社会的、人事的、法制的、物理的、逻辑的和其它方面的安全内容,但归根到底,是逻辑安全中的密码加密在起着支柱作用。

在许多政府部门和大企业工作过程中，资料收集和指令下达高度依靠计算机网络系统,而大量的信息资源存贮于计算机网络上。由此带来了内部信息管理的新问题,主要有:

1)电子保密文档等网络资源的管理问题,传统的保密材料以印刷品的形式存在,可以由专人负责保管,有关人员按规定办理借阅手续,阅后归还,但对存贮于计算机网络中的电子文档显然不适用,如何对电子文档进行管理,需要相应的信息安全技术来支持;

2)相关人员在计算机网上进行的一切活动,包括对有密级的文件的调阅、对下属发布的指令等,应该有详细的审计记录,确保事后有据可查;

3)没有技术手段对特定用户和特定保密信息的访问进行记录,一旦出现泄密事故后不易追查,同时也无法防止抵赖;

4)更严重的外部威胁有,非法访问数据库信息;恶意破坏数据或未经授权非法修改数据;用户通过网络进行数据调用时受到各种攻击(如搭线窃听等)。

对抗外部威胁,加强内部管理,仅仅采用操作系统和网络中的保护是不够的,因为它的结构与其它系统不同,含有重要程度和敏感级别不同的各种数据,并为拥有各种特权的用户共享,同时又不能超出给出的范围。它涉及的范围更广,除了对计算机、外部设备、联机网络和通信设备进行物理保护外,还要采取访问控制和加密技术,防止非法访问或盗用机密数据[1~2];对非法访问的记录和跟踪,同时要保证数据的完整性和一致性等。

存贮数据的加密与通信情况的加密有很大不同:如破译其加密算法所需的密码分析时间仅由数据的价值限定[1];数据可能在另外的盘上、另一台计算机上或纸上以明文形式出现;密码分析者有更多的机会实施

收稿日期:2002-04-18
基金项目:军队科研基金资助项目
作者简介:赵全习(1965-),男,陕西凤翔人,副教授,硕士,主要从事密码学研究.

已知明文破译;在数据库应用中,一串数据可能小于加密分组长度,而造成密文大于明文(数据扩展);输入/输出速度要求实现快速加/解密(因而可能用硬件加密器件来实现);密钥管理更为复杂,因为不同的人要访问不同的文件,或同一文件的不同部分等。

2 存贮数据加密的设计

对系统的存贮数据流加解密时使用 IDEA 类算法[2,5],它极易于软件实现,而且处理时间极短。会话密钥由用户选定或由系统分配,可在较长时间内专用,要求它既安全又易于更换,去启动和控制某种算法(IDEA 算法)所构造的密钥产生器,得到存贮数据所需要的密钥流。根据文件的长度选择是否进行压缩,从文件的使用范围确定是否加上密钥信封。

存贮数据加密过程如图 1 所示,具体步骤如下:

1)用户选择会话密钥 K_Y(例如文件的名称、建立的时间等)并记忆或保存;

2)对明文根据需要确定是否进行压缩,若必要,则用压缩算法(如 ZIP)进行压缩;

3)使用加密算法(如 IDEA)在会话密钥 K_Y 下对欲存贮的数据加密,产生密文;

4)判断是否需要密钥信封(即是否对会话密钥进行加密),若必要,则以使用者公钥 Ku 按 RSA[4] 体制对会话密钥加密,接于密文之后;

5)将密文信息存贮于计算机内或磁盘上,把文件及密钥删除。

解密的步骤只需将此过程逆转,但是打开数字信封时必须用使用者私钥 K_V,具体如图 2 所示。

应该注意,计算机上删除文件,常常是删去了文件名的第一个字母而不能检索,但文件内容仍存在原处,

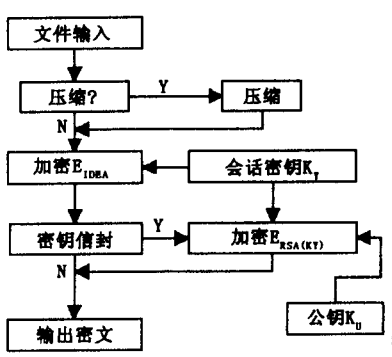

图 1 存贮加密流程图

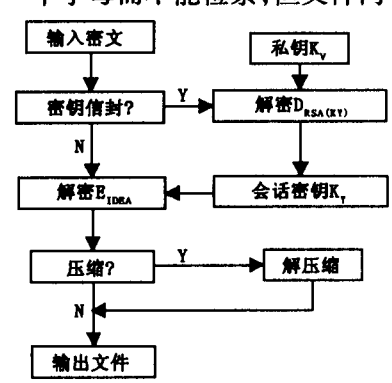

图 2 存贮解密流程图

直到新的数据存入将其覆盖为止,在此之前用文件恢复软件就可以检出。因此,真正从存贮器中删除所存贮的内容需用物理上的重复写入方法。

3 存贮加密系统分析

3.1 强大的文件加密功能

采用目前通用的加密体制——分组密码的杰出代表 IDEA 类加密算法,对文件数据提供加密,算法采用密码反馈(CFB)模式,会话密钥一次性使用,一次一密具有最强的安全性,未授权的用户不仅无法知道文件内容,甚至连文件名也无法知道,增强了数据保密功能。IDEA 算法使用 64 bit 分组 128 bit 密钥,在今后相当长的时间是安全的,除非在该算法中找到根本性的漏洞,或十分奏效的密码分析方法,否则唯一的破译途径就是穷尽搜索全部的密钥。在现有的技术条件下,搜索整个密钥空间,共计 2^{128} 把密钥,是完全行不通的。

采用目前世界上先进的加密体制——RSA 公钥密码体系进行密钥保护,RSA 公开密钥加密的安全性完全依赖于分解大数问题,对于 1 024 模数的 RSA,计算机分解大约需要 10^{10} 年。

3.2 可选的密钥管理功能

提供了两种文件加密方法:"密码加密"和"密钥信封加密"。密码加密不需要 RSA 公钥私钥,加密的文件只有知道密钥的人才能打开。这种加密方法可用于个人处理文件,也可用于加密备份的 RSA 密钥。密钥

信封加密使用分组体制与公钥体制相结合的加密技术对文件加密,可授权多人有解密文件的权利,只有被授权的用户才能解密文件,具有加密共享功能。

密钥信封加密还能提供安全电子邮件功能,加密后的文件作为电子邮件发送出去,只有合法的收件人才能用私钥解密阅读。

3.3 保证了实时性

本系统采用IDEA类和RSA相关算法的混合加密方式,它使两种密码体制的优缺点在一定程度上可相互弥补。使用RSA方式加密会话密钥,不必分配密钥,且保密管理的密钥量也较少,对文件数据流加解密时使用IDEA类算法,处理时间极短,这样在存贮长文件时RSA算法处理会话密钥的时间可以忽略不计。为了进一步提高加解密速度,可以采用对需要处理的文件信息进行分类,对不同类的信息使用不同轮的加密。例如绝密类的信息,采用8轮IDEA类体制加密,实时性强的一般数据,采用4轮乃至更少轮的IDEA类体制加密,加解密速度可比8轮时成倍提高。

3.4 易实现功能平滑引入

加解密模块具有相对的独立性,且都易于采用软件或独立的DSP及硬件实现。增加加解密模块不会影响系统原有的功能及组成方式。以IDEA算法的软件实现为例,加密算法的实现采用C语言,64个寄存器采用C语言的数组类型来实现,IDEA类的大量非线性变换、线性变换都可用C语言的数组操作实现,能够与WINDOWS操作系统紧密结合,操作方便。

4 结论

利用高强度的数据加密技术设计的存贮加密系统,可以有效地保证存贮的信息不被泄露和不被破坏,对文件存贮和电子通信提供了安全可靠的保密功能,此方案对政府部门、企业用户和个人用户构建安全办公环境提供了良好借鉴。

参考文献:

[1] 王育民,刘建伟. 通信网的安全——理论与技术[M]. 西安:西安电子科技大学出版社,1999.

[2] Bruse Schneier. 应用密码学——协议算法与C源程序[M]. 北京:机械工业出版社,2000.

[3] 赵全习,陈西宏,冯有前. 利用IDEA算法之MA——结构的对合置换[J]. 空军工程大学学报(自然科学版),2001,2(3):48-52.

[4] David Pointcheval. 基于RSA相关问题的新公钥加密系统[A],98欧密会议论文精选[C]. 北京:机械工业出版,1998,17-19

[5] Meier W. On the security of the IDEA block[A]. Advances in Cryptology - EUROCRYPT93 Proceedings[C]. Berlin:Springer-Verlag, 1994,22-27.

(编辑:田新华)

Store Data Encryption System Based on IDEA Algorithm

ZHAO Quan-xi, SONG Changn-ping, LIU Hong

(The Missile Institute, Air Force Engineering University, Sanyuan 713800, Shaanxi, China)

Abstract: Inside leak and outside threat in store data have been analyzed in this paper. For the sake of preventing the store data from leaking and filching, by combining with IDEA (encryption algorithm), a store data encryption system is designed. This analysis shows that the system is provided with reliable security, nice key management for selection, good real-time characters and realizability.

Key words: security of information; IDEA; data encryption; RSA