文章编号：1000－5471(2007)04－0068－04

信息存储安全防护系统设计①

林 鹰[1,2]， 苏日娜[1]

1. 重庆交通大学 管理学院，重庆 400074；2. 天津大学 电子信息工程学院，天津 300072

摘要：信息存储安全是信息安全的重要领域，针对计算机内重要文件泄密和存储介质残存信息泄密两大问题，采用文件加密和文件信息完全清除(包括存储介质残余信息清除)两级防范措施，辅以必要的密钥生成、系统设置、防止误操作等系统管理与设置功能，很好的解决了计算机内重要文件泄密和存储介质残存信息泄密问题，系统完整、健壮、高效、易用，完全达到了部队等高保密单位对信息安全的要求.

关 键 词：信息存储安全；文件加密；文件清除

中图分类号：TP309 **文献标识码**：A

随着计算机信息系统的应用日趋广泛，对于信息安全要求较高的部队等高保密单位，加强信息安全防护工作已刻不容缓. 在信息的获取、存储、处理、传输、显示及应用等各个环节，均存在信息安全防护问题，目前安全防护产品大多是用于信息传输、处理和显示环节，事实上，信息存储的安全防护比信息传输和处理时的安全防护更为重要，因为再安全的防火墙都会被攻破；机要加密设备不可能随处可用；网络传输安全并不能保证通过磁盘进行信息交换的安全；强制隔离办公用微机(网络)和家庭用微机(互联网)的管理措施很难长期奏效；机要加密设备由于固定加密算法和密钥，一旦保管不善，就要整批更换，否则就可能造成信息泄密. 因此，在信息存储环节搞好安全防护至关重要，对于提高信息安全防护能力，具有重大的现实意义.

对于各种重要数据信息，必须有非常严格的保密措施，在信息化建设的背景下，信息存储安全防护系统是各级机关的迫切需求. 文章针对计算机内重要文件泄密和存储介质残存信息泄密两大问题，介绍了信息存储安全防护系统设计的总体思路和系统应用的主要技术原理，并据此设计了信息存储安全防护系统的组成和功能，系统完整、健壮、高效、易用，很好的解决了计算机内重要文件泄密和存储介质残存信息泄密问题.

1 系统设计总体思路

信息存储安全防护系统是针对以计算机为载体的各种机要文书、重要数据的安全防护、彻底销毁的需求进行开发的应用系统. 系统的建立遵循以下原则：以需求为出发点，以先进的加密算法为基础，以简便的操作为前提，以用软件工程学方法为依托，建立一个完整、健壮、高效、易用的系统. 系统的目标是：对重要数据进行加密，对不需要保留的数据进行完全销毁，对硬盘空闲磁盘空间进行清理.

系统设计在深入研究信息存储原理和现代密码学的基础上，采用创新或改进的多种加密算法、随机数

① 收稿日期：2006－12－28
基金项目：国家自然科学基金资助项目 (60603027).
作者简介：林 鹰(1962－)，男，重庆人，副教授，主要从事计算机系统、信息工程及智能自动化方向的教学和科研工作.

及密钥生成算法和数据清除算法，实现信息存储的安全防护功能. 包括对各类文件的加解密，对无用文件和数据的彻底删除，对空闲存储介质的清理等功能. 系统是一个纯软件系统，具有加密算法多样、密钥生成安全(随机性好；长度可变；多重组合使用)、功能齐全、执行速度快、操作使用简便(与 Windows 操作系统完全整合)、适用面广等特点.

2　系统的主要原理

2.1　文件加密原理

文件加密就是对原来为明文的文件按照某种算法进行处理，形成不可读的一段代码(通常称为“密文”)，使其只能在输入相应的密钥之后才能显示出原来的内容，通过这样的途径来达到保护文件数据不被非法窃取、阅读的目的.

加密技术通常分为两大类：“对称式”和“非对称式”. 对称式加密就是加密和解密使用同一个密钥；非对称式加密通常有两个密钥，称为“公钥”和“私钥”，必需配对使用才能打开加密文件[1]. 这里的“公钥”是指可以对外公布的，“私钥”则不能，只能由持有人一个人知道. 因为对称式的加密方法如果是在网络上传输加密文件就很难把密钥告诉对方，不管用什么方法都有可能被别人窃听到. 而非对称式的加密方法有两个密钥，且其中的“公钥”是可以公开的，也就不怕别人知道，收件人解密时只要用自己的私钥即可以，这样就很好地避免了密钥的传输安全性问题.

2.2　文件清除原理

文件删除后，在文件所在区块内填充随机数，以达到不可恢复的目的.

2.3　空闲磁盘空间清理原理

对于普通删除的文件，硬盘上还存在有可以恢复的信息，空闲磁盘空间清理就是删除这一遗留信息.

2.4　加密方式配置

加密方式主要有口令加密、密钥盘加密 2 种方式，还可以通过配置，组合使用多个密钥盘和口令，以适应各种使用目的[2].

3　系统的组成

信息存储安全防护系统针对以计算机为载体的各种数据进行安全防护. 主要由文件加解密、文件完全清除、空闲磁盘空间清理、加密方式配置等组成.

4　系统的功能

4.1　信息安全功能

针对数据文件安全，对文件进行加密解密以及直接执行加密文件操作.

4.1.1　文件加密

可以对任意文件及目录加密；可以任意选择加密算法，通过口令或(和)密钥盘，以及二者的多重组合进行加密；与操作系统紧密结合，可以在 WINDOWS 下任意文件管理程序(如资源管理器)中使用鼠标右键呼出的属性菜单命令对文件及目录加密.

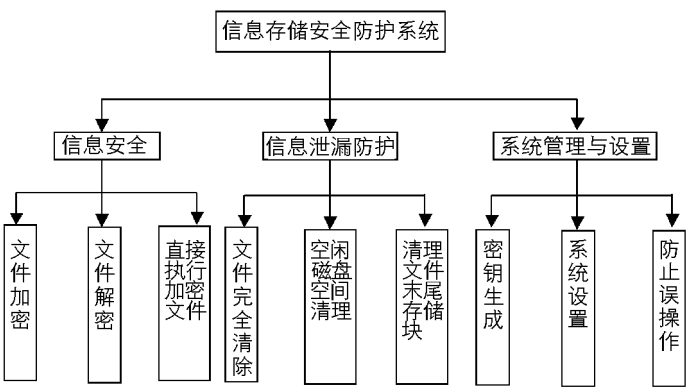

图 1　信息存储安全防护系统总体结构图

4.1.2　文件解密

使用口令或密钥盘对文件或目录进行解密操作；使用鼠标右键呼出的属性菜单命令对文件及目录

解密.

4.1.3 直接执行加密文件

首先对加密文件(如.DOC文件)进行解密,然后自动调用与该文件关联的应用程序(如WORD)来打开该文件并编辑修改,在关闭应用程序后,自动对该文件进行加密.该功能极大地方便了软件操作.

4.2 信息泄漏防护功能

为防止信息泄漏对文件或存储器进行彻底的、不可恢复的清理操作.

4.2.1 完全清除文件

文件通过操作系统删除后,其全部的数据部分还保留在存储器中,通过一定的方法或用一些软件很容易恢复文件,不知情的情况下很容易泄密,而本功能在删除文件的同时,使用随机数据重写该文件的存储块从而达到完全清除文件的目的.

4.2.2 清理空闲磁盘空间

使用多种形式的随机数或固定数字填充空闲磁盘空间.本功能主要对废旧、上交、长时间不用的存储器的空闲空间进行清理,在空间上填充随机数或固定数,覆盖普通删除文件的数据块,使空闲空间的数据不能被恢复.

4.2.3 清理文件末尾存储块

文件是按存储块为单位进行存储的,通常最后一个存储块不会被完全使用,而会留下一部分空闲空间.这个空间可能会保留一些敏感和涉密信息,由于该存储块已经被分配使用,所以利用上述清理空闲磁盘空间功能不能删除这部分信息;而文件加密功能只对文件内容加密,也不能有效地保护这个空闲空间的信息.所以需要设计专门功能来清理一个文件末尾存储块的空闲空间.

4.3 系统管理与设置功能

对系统的密钥、界面、操作以及相关属性进行设置.

4.3.1 密钥生成

可生成1～1024bit的密钥,密钥保存为数据文件,可以放在软磁盘、硬盘、优盘和IC卡等各种存储介质中,只需要在系统使用前指定存储器位置,即可使用.系统设计了一种独特、简便而有效的密钥生成方法:生成密钥文件以前通过鼠标任意移动或敲击键盘来产生1～1024bit的随机数种子.为了保证随机数的质量,程序专门设计了鼠标移动相似性检测算法,其基本思想为:如果移动有重复或相似,则舍弃相应的随机数位,密钥生成过程放慢,反之,鼠标移动的随机性越大,密钥生成得越快.

4.3.2 系统设置

进行加密算法、随机数生成算法以及清除算法的选择;对加密文件的外部特征(文件命名、图表等)进行设置;设置系统的界面效果以及操作方式等.

4.3.3 防止误操作

防止误操作删除、重命名而设置的操作确认口令,提高了系统的实用性.

5 总 结

本系统设计借鉴了以往的经验,采用比较先进的加密算法,随机数产生算法,文件清除算法对数据文件进行加密,保证了技术的先进性,并且紧扣实际工作的需要,减轻了工作人员的工作强度,更有效的保护了数据的安全,系统操作简单,实用性强.改进了数据安全防护手段,提高了业务质量,能够很好的满足信息存储安全防护需要.通过对数据进行安全的加密,减少了常规保密工作的各种开支.系统在极少占用系统资源的情况下,实现了海量数据的加密,有较高的推广价值,且实现的多种算法具有较高的先进性.

参考文献：

[1] Bruce Schneier. 应用密码学[M]. 北京：机械工业出版社，2000.

[2] 中国信息安全产品测评认证中心. 信息安全理论与技术[M]. 北京：人民邮电出版社，2003.

Design of Information Storage Security System for Protection

LIN Ying[1,2]，SU Ri-na[1]

1. School of Management，Chongqing Jiaotong University，Chongqing 400074，China；

2. School of Electronic and Information Engineering，Tianjin University，Tianjin 300072，China

Abstract：Information storage security plays an important role in information security fields. To solve the problems of important document divulged and storage media remaining information divulged inside the computer，this paper adopts the document encryption and the document information complete clearance (include storage media remaining information clearance) technique to design the information storage security system for protection，with necessary function for system management and setting such as generating the key employed in the encryption，system setting，preventing the false operation. The system is integrity，robust，efficient and easy to use. It completely comes to request of information security for the unit such as the troops etc.

Key words：information storage security；document encryption；document clearance

责任编辑　张　枸