(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102609667 A
(43)申请公布日 2012.07.25

(21)申请号 201210040703.8

(22)申请日 2012.02.22

(71)申请人 浙江机电职业技术学院
地址 310053 浙江省杭州市滨江区滨文路528号

(72)发明人 任达千 张伟中 孟庆波 程文锋

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 林怀禹

(51)Int.Cl.
G06F 21/22(2006.01)
H04L 29/06(2006.01)

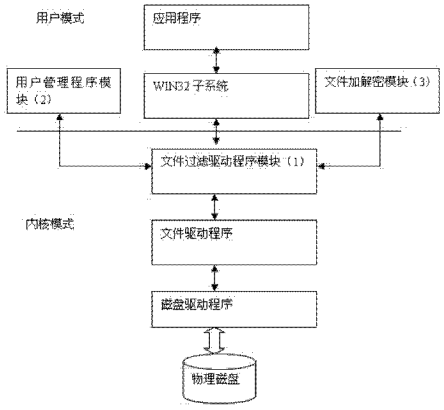
权利要求书 1 页 说明书 3 页 附图 3 页

(54)发明名称

基于过滤驱动程序的文件自动加解密系统和方法

(57)摘要

本发明公开了一种基于过滤驱动程序的文件自动加解密系统和方法。包括Windows操作系统中已有的WIN32子系统、文件驱动程序、磁盘驱动程序和物理磁盘；在WIN32子系统和文件驱动程序间增加一个文件过滤驱动程序模块、用户管理程序模块和文件加解密模块；文件过滤驱动程序模块位于文件驱动程序的上方，文件过滤驱动程序模块分别与用户管理程序模块和文件加解密模块相连，该系统安装在每一个客户端中。加解密系统能拦截所有对加密文件的操作，能自动实现文件加密和解密，对于有足够权限的用户，不会感觉到文件加密系统的存在。文件加密系统在一个局域网内运行，加密文件即使泄露到局域网外，也无法解密。



CN 102609667 A

1. 一种基于过滤驱动程序的文件自动加解密系统，包括 Windows 操作系统中已有的 WIN32 子系统、文件驱动程序、磁盘驱动程序和物理磁盘；其特征在于：在 WIN32 子系统和文件驱动程序间增加一个文件过滤驱动程序模块（1）、用户管理程序模块（2）和文件加解密模块（3）；文件过滤驱动程序模块（1）位于文件驱动程序的上方，文件过滤驱动程序模块（1）分别与用户管理程序模块（2）和文件加解密模块（3）相连，该系统安装在每一个客户端（6）中。

2. 根据权利要求 1 所述的一种基于过滤驱动程序的文件自动加解密系统，其特征在于：所述的每一个客户端（6）通过局域网与服务器（5）连接。

3. 根据权利要求 1 所述的一种基于过滤驱动程序的文件自动加解密系统，其特征在于：所述的客户端（6）的文件过滤驱动程序模块（1）对文件的读、写操作进行拦截。

4. 根据权利要求 1 所述系统的一种基于过滤驱动程序的文件自动加解密的方法，其特征在于：

1）当客户端对文件进行读操作时，文件过滤驱动程序模块（1）读取文件的加密数据块（4）中的数据，判断是否为加密文件，如果是加密文件，则取得加密算法，再从服务器（5）取得加密文件的权限、文件类型、文件合法用户这些信息，然后调用文件加解密模块（3）对文件进行解密，然后调用文件驱动程序读取文件，如果不是加密文件，则文件过滤驱动程序模块（1）调用文件驱动程序读取文件；

2）当客户端对文件进行写操作时，文件过滤驱动程序模块（1）取得应用程序的名称、文件类型这些信息，判断是否需要加密，如果需要加密，则生成加密数据块（4），然后调用文件加解密模块（3）加密文件，再写入磁盘，调用用户管理程序模块（2），将加密文件的加密信息发送到服务器（5）保存，如果不需要加密，则调用文件驱动程序写文件。

基于过滤驱动程序的文件自动加解密系统和方法

技术领域

[0001] 本发明涉及一种加解密系统和方法，尤其是涉及一种基于过滤驱动程序的文件自动加解密系统和方法。

背景技术

[0002] 计算机文件加密技术广泛应用于各领域。比如在制造业领域，各种图纸、文档均存储在计算机中。这些图纸、文档是技术人员艰苦劳动的成果，也是企业重要的生产资料，并且可以为企业创造价值，因此需要有足够的保护措施。为了利用这些图纸、文档，又需要有拷贝、编辑、打印等操作，很多情况下也需要在一个局域网内传输。文件加密系统的功能是保护文件，既不影响对文件的正常操作，又能防止被非法访问、利用。

[0003] 目前文件自动加解密系统的实现方法主要是应用层加密技术，即 HOOK 技术，在应用程序调用文件操作函数时，比如打开、关闭文件，读写文件时均会调用一个 HOOK 程序，在 HOOK 程序中即可对文件进行加密和解密。这种加密技术比较容易实现，但是因为其原理的缺陷，容易被一些事先潜伏的木马病毒截获。这种技术的适应性较差，同时加密多种应用程序时相互干扰大。

发明内容

[0004] 本发明的目的在于提供一种基于过滤驱动程序的文件自动加解密系统和方法，驱动层加解密技术是通过设计一个文件过滤驱动程序模块，实现自动加密和解密功能，控制更加灵活，运行更加稳定。

[0005] 本发明采用的技术方案是：

一、一种基于过滤驱动程序的文件自动加解密系统：

本发明包括 Windows 操作系统中已有的 WIN32 子系统、文件驱动程序、磁盘驱动程序和物理磁盘；在 WIN32 子系统和文件驱动程序间增加一个文件过滤驱动程序模块、用户管理程序模块和文件加解密模块；文件过滤驱动程序模块位于文件驱动程序的上方，文件过滤驱动程序模块分别与用户管理程序模块和文件加解密模块相连，该系统安装在每一个客户端中。

[0006] 所述的每一个客户端通过局域网与服务器连接。

[0007] 所述的客户端的文件过滤驱动程序模块对文件的读、写操作进行拦截。

[0008] 二、一种基于过滤驱动程序的文件自动加解密的方法：

1）当客户端对文件进行读操作时，文件过滤驱动程序模块读取文件的加密数据块中的数据，判断是否为加密文件，如果是加密文件，则取得加密算法，再从服务器取得加密文件的权限、文件类型、文件合法用户这些信息，然后调用文件加解密模块对文件进行解密，然后调用文件驱动程序读取文件，如果不是加密文件，则文件过滤驱动程序模块调用文件驱动程序读取文件；

2）当客户端对文件进行写操作时，文件过滤驱动程序模块取得应用程序的名称、文件

类型这些信息，判断是否需要加密，如果需要加密，则生成加密数据块，然后调用文件加解密模块加密文件，再写入磁盘。调用用户管理程序模块，将加密文件的加密信息发送到服务器保存，如果不需要加密，则调用文件驱动程序写文件。

[0009] 本发明有益的效果是：

本发明在一台加解密服务器上对同一局域网内计算机上的文件进行分类管理，可设置不同的加解密等级，不同的访问权限。在驱动层截获应用程序对文件的操作，对文件的任何操作都无法被绕过。增加了文件加解密系统的可靠性。具有访问权限的用户，在访问文件时自动加解密，因此对加密文件的访问与普通文件完全一样，不会感觉到文件加解密系统的存在。没有访问权限的用户，则只能得到文件密文，无法获取文件明文。文件如果流出局域网，则无法对文件进行解密，无足够权限的用户即使得到文件，也无法利用加密文件。驱动层加解密技术控制更加灵活，运行更加稳定。过滤驱动程序涉及到 Windows 系统内核，技术门槛较高，核心技术仅被少数几家实力雄厚的公司所掌握，不容易被攻击。因此基于过滤驱动程序的文件加密技术是一种很有发展前景的加密技术。

附图说明

[0010] 图 1 是自动加密系统局域网组成图。

[0011] 图 2 是 Windows 系统文件存取方式示意。

[0012] 图 3 是文件自动加密系统的结构图。

[0013] 图 4 是加密文件格式图。

[0014] 图 5 是读文件流程图。

[0015] 图 6 是写文件流程图。

具体实施方式

[0016] 下面结合附图和实施例对本发明作进一步说明。

[0017] 如图 1 所示，是自动加密系统局域网组成图。每一个客户端 6 通过局域网与服务器 5 连接。服务器 5 上设置有加密文件数据库，包括每个加密文件的加密权限、加密算法等信息。当客户端 6 向物理磁盘上写加密文件时，将自动加密，并将相关信息保存到服务器 5 上。客户端 6 在读物理磁盘上的加密文件时，将向服务器 5 取得该文件的权限、加密算法等信息，对于具有足够权限的用户，客户端 6 将自动解密文件。

[0018] 图 2 为 Windows 操作系统的文件系统示意图，这里所指的应用程序包括常见的 Word、Excel 等办公软件，在制造业领域所使用的 AutoCAD, ProE, Protel 等软件。应用程序读写文件时，首先调用 WIN32 子系统，比如 CreateFile、ReadFile、WriteFile 等系统函数。WIN32 子系统则调用操作系统内核的文件驱动程序，文件驱动程序进一步调用磁盘驱动程序完成对物理磁盘的访问。应用程序和 WIN32 子系统运行于操作系统的用户模式，文件驱动程序和磁盘驱动程序运行于操作系统的内核模式。

[0019] 如图 3 所示，文件自动加解密系统在现有 Windows 操作系统的文件系统基础上，增加了 3 部分程序模块，分别为文件过滤驱动程序模块 1、用户管理程序模块 2 和文件加解密模块 3。其中文件过滤驱动程序模块 1 位于操作系统的内核，可以拦截、过滤任何对文件驱动程序的调用，即 WIN32 子系统对文件驱动程序的任何调用比如文件打开、关闭、读、写等

操作均先经过文件过滤驱动程序模块 1。当应用程序读、写加密文件时，文件过滤驱动程序模块 1 即逆向调用用户管理程序模块 2，用户管理程序模块 2 将文件的使用用户、管理权限、加密等级等信息通过局域网发送到服务器 5 上，再根据返回的信息判断是否对文件进行加密、解密操作。文件加解密模块 3 则是一个动态加载模块，主要是自主开发的加解密算法的程序实现，也包括各种常见的加解密算法如 MD5、DES 和 RSA 等的程序实现，供文件过滤驱动程序程序模块 1 调用。因此本发明公开的文件加解密系统可以根据用户需要选用不同的加密算法。如上所述，对三部分程序做了不同的分工，文件过滤驱动程序模块 1 是运行于内核模式，开发、调试都比较困难，而对运算速度的要求较高，因此文件过滤驱动程序模块 1 只实现最必须的功能。网络通讯、用户界面等功能均在用户管理程序模块 2 实现。文件加解密模块 3 主要是复杂的加解密算法，在用户模式下，有利于开发、调试和修改。

[0020] 如图 4 所示，未加密的文件为明文，加密文件包括加密数据块 4 和密文。加密数据块 4 位于加密文件头部，是一个 4K 字节大小的数据块，为使加密系统可以使用多种加密方法，在加密数据块 4 中保存加密标记、加密等级、加密算法标记、密钥等信息。文件头部之后是文件的密文，因加密算法的不同，密文长度可以与明文长度相等，也可以不相等。

[0021] 读取加密文件的流程图，如图 5 所示，当用户程序读取一个加密文件时，比如办公软件 Word 程序读取一个 *.doc 文件，当过滤驱动程序拦截这个读取操作时，先读取文件头部 4K 字节的加密数据块，判断是否加密文件，并识别加密所用算法等，对于非加密文件，则调用文件驱动程序，完成文件读取。对于加密文件，文件过滤驱动程序模块 1 逆向调用用户管理程序模块 2，用户管理程序模块 2 通过局域网获取服务器 5 上的加密文件权限、加密算法等信息，文件过滤驱动程序 1 接着再调用加解密模块 3 完成文件的解密。如果客户端 6 的用户没有足够的权限，则不解密文件，直接返回密文文件。

[0022] 如图 6 所示，当文件过滤驱动程序模块 1 拦截到写文件操作时，将取得应用程序的名称、文件类型等信息。接着判断是否需要加密，加密完成后调用文件驱动程序将文件写入磁盘。再调用用户管理程序模块 2，将加密文件的加密信息发送到服务器 5 保存。写文件的操作即告完成。

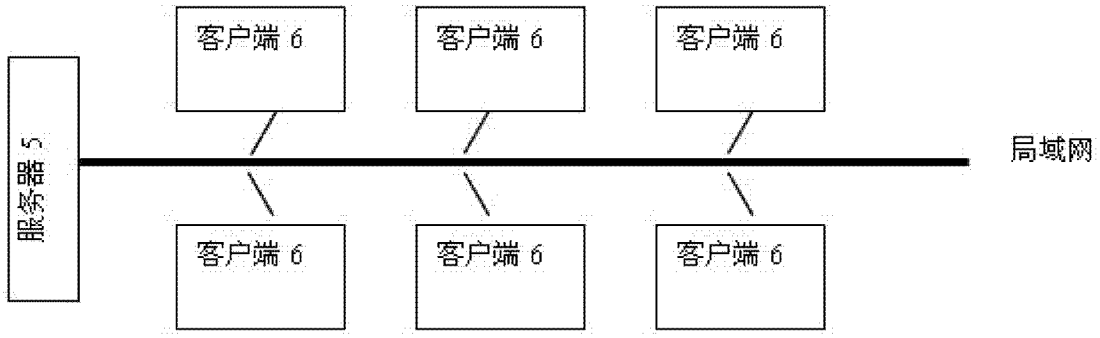

服务器 5
客户端 6
客户端 6
客户端 6
客户端 6
客户端 6
客户端 6
局域网

图 1

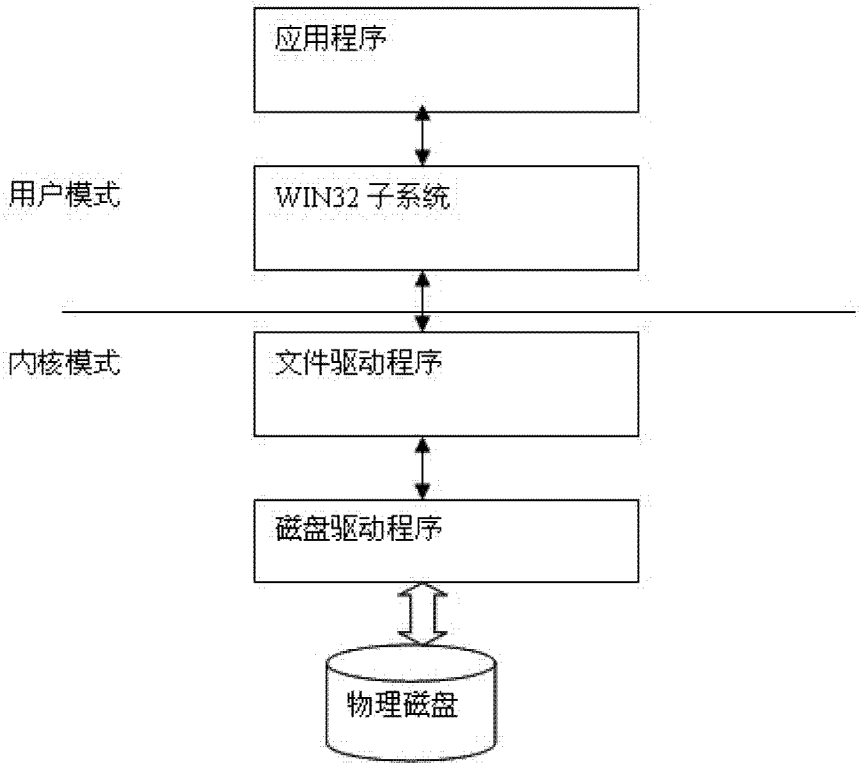

应用程序
用户模式
WIN32 子系统
内核模式
文件驱动程序
磁盘驱动程序
物理磁盘

图 2

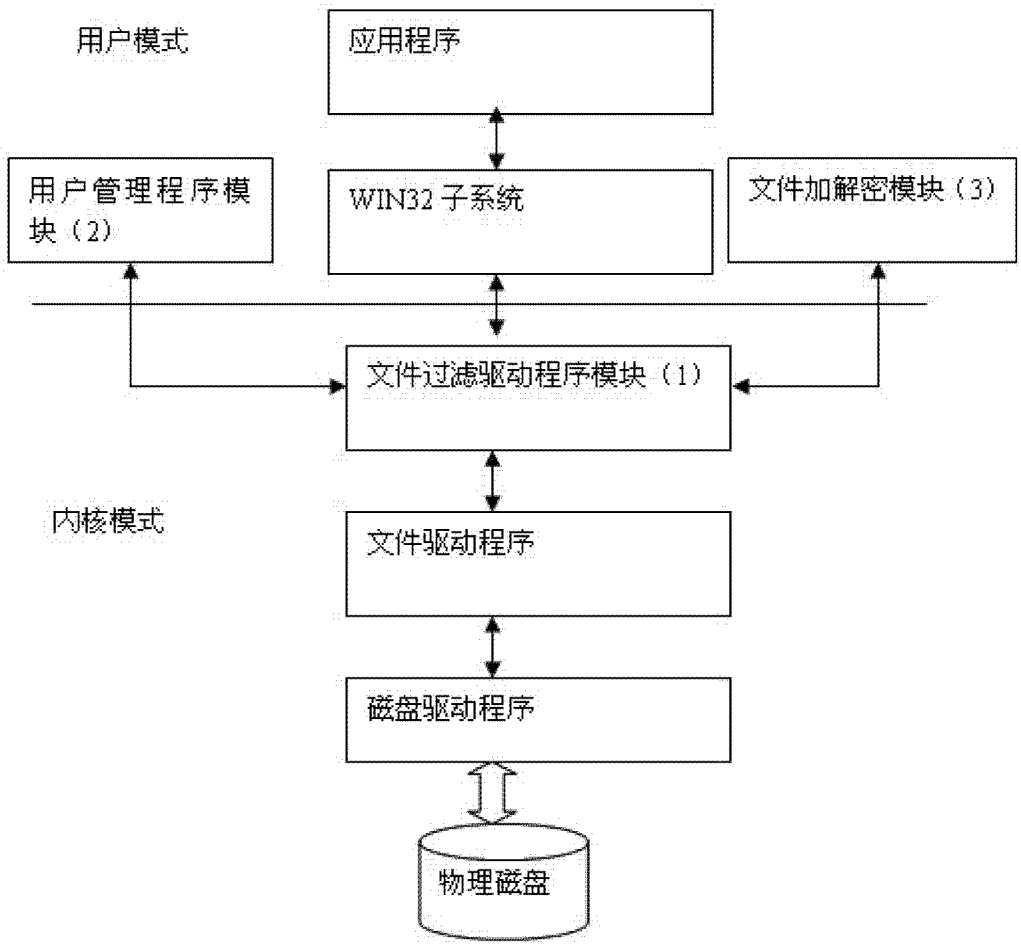

用户模式
应用程序
用户管理程序模块（2）
WIN32 子系统
文件加解密模块（3）
文件过滤驱动程序模块（1）
内核模式
文件驱动程序
磁盘驱动程序
物理磁盘

图 3

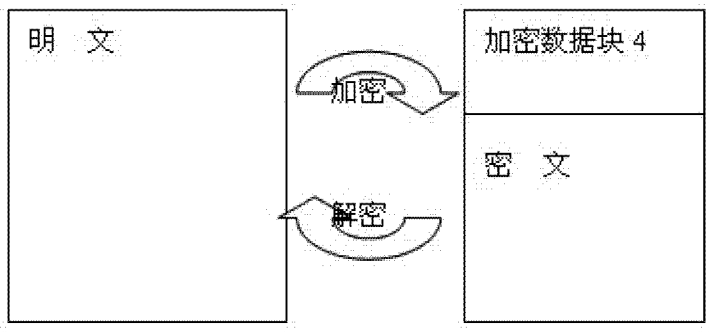

明 文
加密
解密
加密数据块 4
密 文

图 4

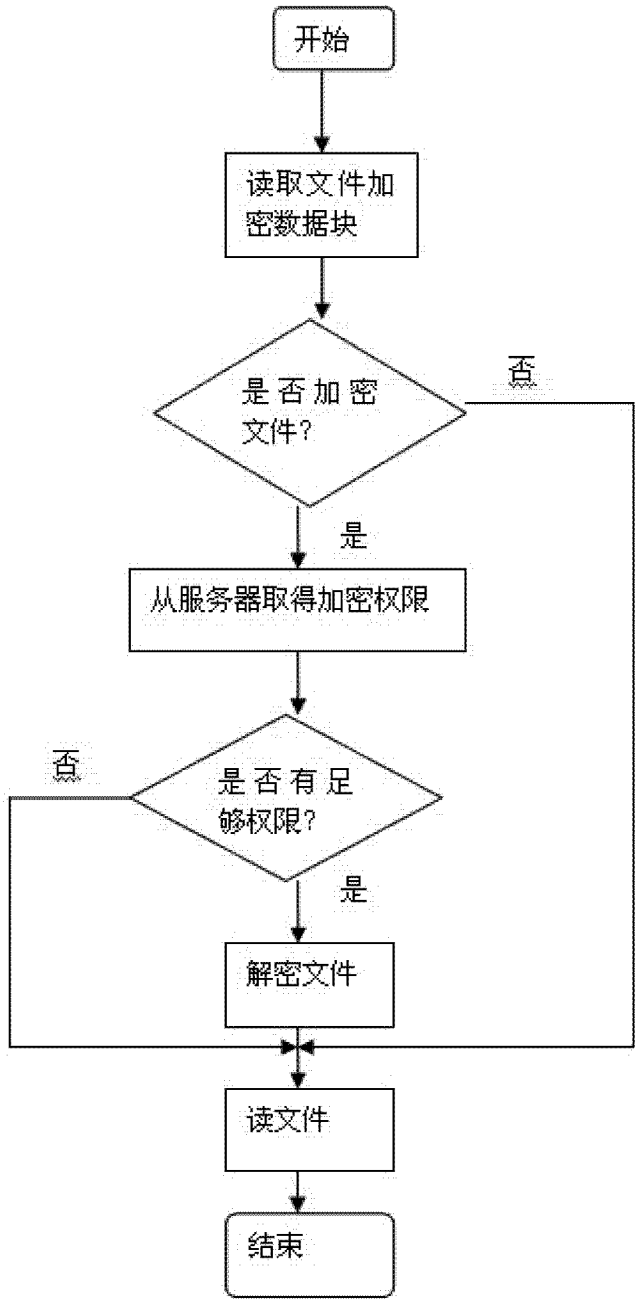

开始
读取文件加密数据块
是否加密文件?
否
是
从服务器取得加密权限
是否有足够权限?
否
是
解密文件
读文件
结束

图 5

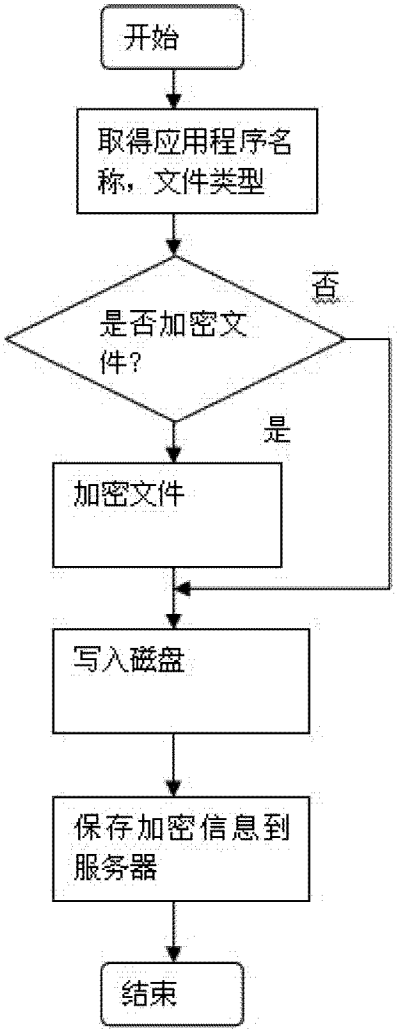

开始
取得应用程序名称，文件类型
是否加密文件?
否
是
加密文件
写入磁盘
保存加密信息到服务器
结束

图 6