

基于隐藏分区的安全优盘系统设计

何 为,于 洋,晁志超

(重庆通信学院 通信指挥系,重庆 40035)

摘 要: 针对优盘遗失、被窃取等情况,提出结合隐藏分区和数据加密的保护方法,利用 USB Composite(USB 组合设备)结构模型,建立了一个隐藏加密分区和一个普通分区,当优盘插入计算机时普通分区可供用户使用;利用上位机软件与优盘动态认证身份,认证成功后可动态挂载隐藏分区,隐藏分区数据通过上位机过滤驱动程序加解密。经过实际测试,安全优盘操作使用简单、隐密性好、加解密速度快,实用有效,达到了预期目标。

关键词: USB 组合设备;身份认证;动态挂载;过滤驱动

中图分类号: TP309.1

文献标识码: A

文章编号: 1000—7180(2017)02—0087—05

Design of Security USB Flash Disk Based on Hidden Partitions

HE Wei, YU Yang, CHAO Zhi-chao

(College of Communication Command, Chongqing Communication College of PLA, Chongqing 400035, China)

Abstract: For lost and stolen USB disk, put forward combining the hidden partition and data encryption protection method, using USB composite (USB composite device) structure model, established a hidden encrypted partition and a regular partition, when USB disk into the computer the ordinary partitions can be for users to use; the use of PC software and USB dynamic identity authentication, the authentication is successful can be dynamic mount hidden partition, the hidden partition data is filtered through the PC driver program encryption and decryption. After the actual test, security USB disk operation using simple, confidentiality good, fast speed of encryption and decryption, practical and effective, to achieve the expected goal.

Key words: USB composite; identity authentication; dynamic mount; filter driver

1 引言

随着信息技术的飞速发展,优盘因其体积小、使用便捷成为最重要的数据中转与存储工具,优盘数据的安全性也已经成为信息安全领域关注的焦点。针对优盘遗失后数据泄密问题,主要技术手段是对优盘数据加密存储,可分为计算机软件加密和优盘硬件加密两种方式。计算机软件加密方式按照实现技术方案不同可分为文件加密和磁盘加密,文件加密针对优盘存储的独立文件、文件夹,而磁盘加密则是针对整个优盘存储区域;文件加密方式多以应用层的软件实现,磁盘加密则以过滤层加密为主。硬件加密是指数据加解密由优盘硬件完成,但加密密钥

验证方式有计算机软件认证、优盘硬件身份认证(优盘自带指纹识别认证或者按键密码认证)。软件加密方式优点是先对数据进行加密,再传输至优盘存储,在数据传输、存储过程均是密文;硬件加密方式其显著优势在于加解密由硬件完成,加解密速度快。

2 系统方案

本方案采用软硬结合的方式设计了基于隐藏分区的安全优盘系统。硬件部分按照 USB 协议应答、主控程序、明盘盘密功能的层次,实现了隐藏分区安全优盘功能,采用 USB 组合设备模型结构,组合了两个 USB Mass Storage 设备、一个 USBKEY 设备,由 USB 主控芯片、存储芯片以及附属电路构成。

计算机端软件采用 Visual Studio 2010 编程实现,由应用层 UDiskCrypt. exe 应用程序和过滤驱动层 UDiskCrypt. sys 驱动程序组成,应用程序实现了系统界面、与用户交互实现身份认证、在操作系统中实现分区隐藏等功能,过滤驱动程序实现了对优盘数据写读的加解密功能以及隐藏安全分区格式化、挂载卸载等功能,系统结构示意图如图 1 所示^[1].

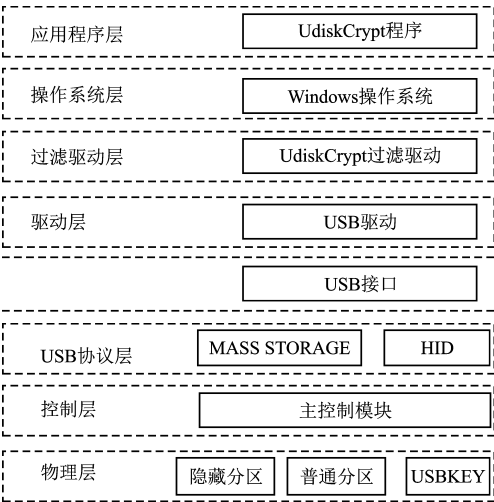


图 1 系统结构示意图

系统的工作流程设计：

- (1)当优盘插入计算机时,经过 USB 协议枚举、应答等环节,一个普通分区和 USBKEY 设备直接挂载到操作系统中,其中普通分区和市场上的普通优盘一样,直接供用户使用；
- (2)上位机 UDiskCrypt. exe 应用程序启动后,与隐藏分区安全优盘内部集成的 USBKEY 进行身份认证,确定软件与优盘身份的合法性；
- (3)身份认证通过后,将隐藏分区暴露出来,由于该分区全盘加密,操作系统仅能识别隐藏分区为 RAW 格式(不可识别格式),不能直接使用；
- (4)用户键入对应隐藏分区的加密密码,密码验证成功后,将加密优盘分区映射为虚拟磁盘,挂载到系统中,供用户使用。

3 系统实现

3.1 软件部分

上位机应用程序 UDiskCrypt 是基于对话框的程序^[2-3]. 当 UDiskCrypt 程序启动后,首先检测当前 USB 设备列表指定 VID、PID 设备,查找指定的 USBKEY 设备,而后采用随机数自动与 USBKEY 设备验证身份,更新显示当前状态,等待用户选择相应功能,当前的主要功能有隐藏分区创建、挂载、卸

载和退出等. 其中与隐藏分区数据读写相关的操作将调用过滤驱动程序 UDiskCrypt. sys 完成,该过滤驱动采用核心层(Kernel)透明加密技术实现,是采用基于可安装文件系统(Installable File System)开发接口设计的文件过滤驱动,实现透明加解密功能. 驱动层的透明加解密与操作系统的文件系统结合紧密,加解密效率更高,控制更加灵活,运行更加稳定. 软件系统流程图如图 2 所示.

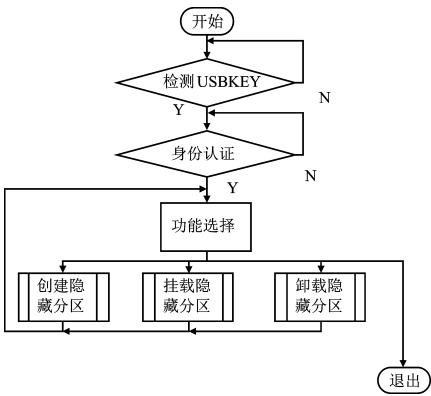


图 2 软件系统流程图

3.1.1 优盘主要操作实现

隐藏优盘的主要操作包括创建隐藏优盘分区、挂载优盘分区、卸载优盘分区,实现方法如下.

(1)创建隐藏优盘分区

创建隐藏优盘分区是按照给定密钥对分区进行格式化,使优盘分区能够正常在操作系统中使用. 有以下几个处理步骤.

- ① 根据输入的用户口令生成加密密钥；
- ② 读取磁盘信息,在内存中创建文件系统头结构(支持 FAT32 和 NTFS 格式)；

磁盘分区内存结构如下：

```
typedef struct
{
    BOOL bDevice; //分区卷标记
    BOOL hiddenVol; //隐藏卷标记
    char * volumePath; //分区卷路径
    unsigned __int64 size; //分区容量大小
    .....(略)
    HWND hwndDlg; //传入窗口句柄
} FORMAT_VOL_PARAMETERS;
```

③ 调用写磁盘命令,创建磁盘分区文件系统,完成格式化,如下：

```
TCFormatVolume(FORMAT_VOL_PARAMETERS
* volParams);
```

(2)动态挂载卸载

挂载是指将隐藏优盘分区挂载到操作系统;卸载是指从操作系统中卸载弹出隐藏优盘分区。

①动态挂卸载

- 用户输入隐藏安全优盘密码;
- 通过过滤驱动程序读取隐藏优盘文件系统相关信息;
- 映射为一个虚拟磁盘分区向操作系统发出新设备检测消息;
- 操作系统重新检测设备发现该虚拟映射分区,挂载该分区,并分配盘符.

挂载实现函数如下:

```
int MountVolume (HWND hwndDlg,           //窗口句柄
char * volumePath,           //分区路径
Password * password,         //用户口令
BOOLcachePassword,          //缓存口令标记
BOOLsharedAccess,           //共享操作标记
MountOptions * mountOptions, //挂载磁盘参数
BOOLbReportWrongPassword) //口令错误报告
```

MountVolume 函数返回结果是: -1 表示用户终止加载;0 表示加载失败;1 表示加载成功;2 表示在共享模式加载成功.

②卸载磁盘

UDiskCrypt 数据加密软件根据用户选择卸载功能.

卸载磁盘构架如下:

```
BOOLUnmountVolume(HWND hwndDlg, //传入的窗口句柄
Int nDosDriveNo, //加载磁盘分区序号
BOOLforceUnmount ) //是否强制卸载
```

3.1.2 文件过滤驱动的实现^[3]

(1)文件加密系统组成

文件加密系统由文件过滤驱动程序和用户模式应用程序组成. 文件过滤驱动程序接收用户模式应用程序发送的信息,对文件系统过滤驱动进行设置;对应用程序发往文件系统的操作请求进行监控;在应用程序对磁盘上的文件进行读操作时,进行相应的处理和解密操作;在进行写操作时,进行加密操作. 如图 3 所示.

(2)文件系统过滤驱动与用户模式应用程序通信

应用程序向驱动程序交互信息时,由应用程序获取设备驱动程序的句柄后,使用 DeviceIoControl()函数来实现与设备驱动程序之间的通信,而文件系统过滤驱动拦截了所有的 I/O 请求,实现过滤功

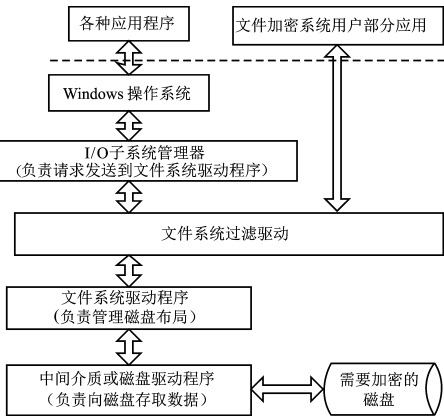


图 3 过滤驱动流程图

能. 因此,文件系统过滤驱动必须区分哪些 I/O 请求需要文件系统过滤驱动处理,采用在驱动入口函数 DriverEntry()中用 IoCreateDevice()创建一个命名控制设备对象,并在该设备扩展 DeviceExtension 中定义设备类型.

在拦截 IRP 请求后,通过检查设备类型判断是否是 GUIINTERFACE,即可知该 IRP 是系统发送的还是用户模式应用程序发送的,也可知该请求是否是发给对应文件系统过滤驱动的. DeviceIoControl()函数通过这些与文件系统过滤驱动控制设备对象名相关联的 I/O 控制码,向文件系统过滤驱动程序传递和接收数据的;文件系统过滤驱动则是通过 IRPMJDEVICECONTROL 分发处理函数或 fastIoDispatch->FastIoDeviceControl 回调函数接收 DeviceIoControl()函数发送的信息. 由此,完成了过滤驱动程序与用户程序的通信过程.

3.1.3 身份认证方法

隐藏加密优盘上位机软件需要与加密优盘之间认证身份认证后,才能将隐藏安全优盘暴露在操作系统中. 身份认证方法由计算机端软件和 USBKEY 设备各种发起一次认证,从而实现双向身份认证. 认证成功后 UDiskCrypt 软件可对安全分区进行后续的挂载、卸载等操作.

(1)检测加密优盘

检测加密优盘是否正常接入是通过检测内部嵌入的 USBKEY 设备是否正常连接实现的. USBKEY 设备是以 HID 协议与计算机通信,在启动上位机软件系统或者当 USB 总线变化时,上位机软件会通过查找指定 VID 和 PID 值,检测 USBKEY 是否已经接入操作系统,若没有则返回无加密优盘接入,由如下函数实现.

```
BOOLOpenHidDevice ( HANDLE * HidDevHandle,
```

//设备句柄

USHORT vid, //VID 值,短整型

USHORT pid, //PID 值,短整型

(2) 身份认证方法

首先由计算机向 USBKEY 设备发起身份认证,步骤如下:

① 生成随机数,发送至 USBKEY 设备;

② 上位机软件对随机数进行计算处理,USBKEY 设备对随机数进行计算处理;

③ 上位机软件比对 USBKEY 返回结果和直接计算结果,完成计算机对 USBKEY 设备的认证.

然后,采用上面相同的方法,由 USBKEY 向上位机软件发起随机数验证,从而实现双向身份认证.通过身份认证后,隐藏安全优盘将会加载隐藏加密分区.

3.1.4 密钥认证方法

在用户需要挂载隐藏安全优盘分区时,需要认证优盘加密密码,本设计没有在中系统中存储密钥,采用验证试探的方法进行密钥验证.也即是通过设置特征字符串,在生成加密优盘分区时,利用用户输入密钥,对特征字符串加密,而后,写入磁盘的特定区域;验证密钥时,使用用户键入密钥对磁盘特定区域数据进行解密,如果得到原始特征字符串,则说明密钥正确.

3.2 硬件部分

3.2.1 硬件电路设计^[4-5]

优盘的电路由主控芯片、存储信息片和必要外围器件组成^[6].在这里,选用了 CYPRESS 高速 USB2.0 芯片 FX2LP CY7C68013A 主控芯片^[7],该芯片内部集成了 USB2.0 收发器、串行接口引擎、增强 8051 微控制器核、8.5 kB 的 RAM 以及 4 kB 容量的 FIFO,支持最大 480MB/s 的传输速度,支持容量 1~4 GB NAND FLASH 存储芯片.采用 IIC 总线,外接 EEPROM 芯片 24LC128 存储微控制器程序;选用三星 NAND FLASH 芯片 K9F1G08U0A 作为存储芯片.

3.2.2 硬件功能程序设计

隐藏加密优盘硬件程序设计以 Keil C 为开发平台,对 Cypress 公司的 CY7C68013A 主控芯片进行编程,基于官方 FX2LP 开发套件^[8],实现了枚举应答、组合结构模型、身份认证应答、读写 FLASH 分区等功能.

(1) 相关描述符

USB 设备使用 USB 描述符向上位机说明主要

功能.USB 上电时,通过多次枚举与上位机交互相应数据,上位机准备相关资源、驱动以便能正常使用该设备.描述符主要分为设备描述符、配置描述符、字符串描述符、接口描述符、端点描述符等.

程序采用 USB Composite 结构,在配置描述符中将接口描述符数量设置为 2,由于一个接口描述符将对应一个设备,因此实现了两个设备功能.其中一个是 HID 接口描述符,按照标准 HID 描述符格式,详细描述了该接口功能,该接口对应 USBKEY 设备;另外一个则是 Mass Storage 大容量存储设备,也即安全优盘,主要包含厂商描述符和 BULK 端点描述符等内容.

(2) 身份认证功能实现

身份认证功能主要用于应答上位机身份验证,或者通过生成随机数验证上位机身份,主要由随机数产生单元和认证单元完成.

① 随机数产生机制

由于单片机运行 rand() 等随机数时,会在编译时将 rand() 值带入,使得所取随机数成为固定值,不利用程序运行,在此设计了一种随机数产生机制.

A 记录单片机程序运行时间周期

在定时器溢出中断服务程序中,累计定时器溢出次数 T.而记每一时刻定时器中数值为 t,则当前单片机运行周期数值可表示为 $256 * T + t$.

B 获取随机数

由于上位机身份认证的时间随机性,记录上位机身份认证的时间点的微控制器运行时间周期作为随机数种子,然后调用随机数函数根据随机数种子,得到随机数.

② 加密验证算法

程序采用 AES 标准加密算法对随机数进行加密运算. AES 加密过程是在一个 4×4 的字节矩阵 (state) 上运作,其初值就是一个明文区块.加密时,各轮 AES 加密循环均包含 4 个步骤: AddRoundKey (轮密钥加变换)、SubBytes (字节代替变换)、ShiftRows (行移位变换)、MixColumns (列混淆变换).具体内容可参见 AES 加密算法标准.

(3) USB Mass Storage 协议实现

USB Mass storage Device 协议即海量存储设备协议适用于硬盘、U 盘等大容量存储设备,使用接口端点有 BulkIn、BulkOut 和 Interrupt 端点,包含多个独立的子类以及传输协议,使用 CBW (Command Block Wrapper) 指令格式,包含为 31 个字节. CBW 中的 bCBWLUN 位设置为 1,使用多个 LUN

逻辑单元的设备,一个设备对应明盘分区,一个对应隐藏分区.采用 SCSI 命令集对存储区域操作,USB Mass Storage 用到的主要指令如下所示.

- Format Unit:格式化存储设备
 - Inquiry:获取设备信息
 - Mode Sense:返回参数
 - Read(10)/Read(12):从设备读取数据
 - Read Capacity:读取设备容量
 - Read Format Capacity:读取当前设备容量和可格式化的容量
 - Prevent/Allow Medium Removal:写保护
 - Request Sense:获取状态信息
 - Seek(10):为设备分配地址
 - Send Diagnostic:硬件复位并执行诊断
 - Write(10)/Write(12):写数据到存储设备
- 针对上述指令,通过在系统中编程,分别编写对应函数进行实现功能.

4 系统性能测试

4.1 测试环境

硬件平台:HP DV4-3115TX 笔记本电脑,处理器 I5-2 410 M(2.3 GHz),500 GB 硬盘,4 GB 内存,Usb2.0;

软件平台:windows7 32 位 操作系统;
测试软件:ATTO DISK bench32(测试速度).

4.2 读写速度测试

在测试环境中正常验证身份后开启隐藏加密分区,使用 ATTO DISK bench32 软件,对隐藏安全分区进行测试,测试结果如图 4 所示.

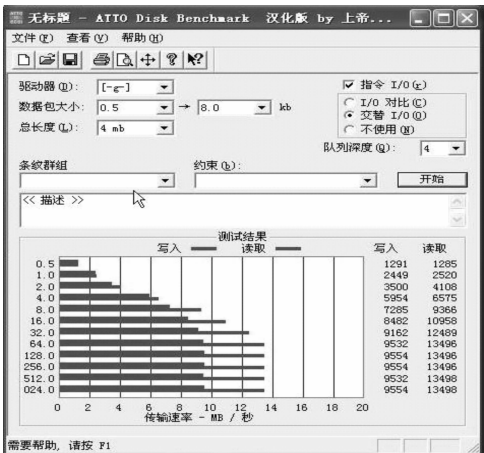


图 4 磁盘读写测试结果

由图 4 可以看出,最大写速度接近 10 MB/s,读速度接近 13.5MB/s.该读写速度与普通 USB2.0

接口优盘的读写速度无明显差别.

4.3 隐藏功能测试

(1)测试过程

① 当优盘插入后,在资源管理器中看到一个 H 盘,也即是普通优盘,隐藏加密分区没有出现.

② 登陆 UDiskCrypt 软件,挂载隐藏安全分区,如图 5 所示.此时,磁盘管理界面中可看到的磁盘 1 和磁盘 2,其对应资源管理器中的 H 盘和 I 盘,也即普通优盘和隐藏安全优盘分区.

卸载加密分区,则隐藏安全优盘从设备管理器中消失.



图 5 功能测试图

(2)结论分析

从上述测试中可以看出,隐藏安全优盘系统能在没有经过身份认证时能很好地隐藏加密分区,而在通过身份认证后,将挂载隐藏加密分区,在使用上,隐藏加密分区与普通分区没有明显差别,到达预期设计功能.

5 结束语

本设计按照 USB Composite 结构模型,结合过滤驱动技术,在一个优盘中集成了一个 HID 类型的 USBKEY 设备、两个 Mass Storage 设备,从外观上实现了加密优盘的隐藏;当上位机程序与优盘 USBKEY 设备通过身份认证后,未通过身份认证则该安全分区处于隐藏状态;身份认证通过后可动态挂载的 Mass Storage 设备并映射为一个虚拟磁盘分区,其中数据通过过滤驱动程序加解密,实现安全优盘的加密存储.通过外观隐藏、数据隐藏的“双重隐藏”的被动防御思路,结合数据加密,对优盘安全提

(下转第 96 页)

取,对提取的特征参量采用变结构神经网络控制器进行伴随跟踪训练,实现数据聚类中心搜索和预测指向性误差的小扰动抑制,完成统计数据时间序列的准确预测.研究得知,采用该算法进行统计数据预测的精度较高,误差较小,内存开销和计算开销等指标参量都具有一定的优越性,展示了较高的应用价值.

参考文献:

[1] 陆兴华,陈平华. 基于定量递归联合熵特征重构的缓冲区流量预测算法[J]. 计算机科学, 2015, 42(4): 68-71.

[2] 杨雷,李贵鹏,张萍. 改进的 Wolf 一步预测的网络异常流量检测[J]. 科技通报, 2014, 30(2): 47-49.

[3] 梁聪刚,王鸿章. 微分进化算法的优化研究及其在聚类分析中的应用[J]. 现代电子技术, 2016, 39(13): 103-107.

[4] Ortiz A, Gorriz J M, Ramirez J, et al. Improving MR brain image segmentation using self-organising maps and entropy-gradient clustering[J]. Information Sciences, 2014, 262(3): 117-136.

[5] 李牧东,赵辉,翁兴伟,等. 基于最优高斯随机游走和个体筛选策略的差分进化算法[J]. 控制与决策,

2016, 31(8): 1379-1386.

[6] 周丽燕,王立洪. 长记忆多项式回归模型的置信域估计[J]. 应用数学学报, 2014, 37(1): 31-44.

[7] 芮兰兰,李钦铭. 基于组合模型的短时交通流量预测算法[J]. 电子与信息学报, 2016, 38(5): 1227-1233.

[8] 李祖雄. 一类具有反馈控制的修正 Leslie-Gower 模型的周期解[J]. 应用数学学报, 2015, 38(1): 37-52.

[9] Din D R, Huang J S. Multicast backup reprovisioning problem for Hamiltonian cycle-based protection on WDM networks[J]. Optical Fiber Technology, 2014, 20(2): 142-157.

[10] Choi J S. Design and implementation of a PCE-based software-defined provisioning framework for carrier-grade MPLS-TP networks[J]. Photonic Network Communications, 2014, 29(1): 96-105.

作者简介:

单冬红 女(蒙古族), (1976-), 硕士研究生, 副教授. 研究方向为数据挖掘、计算机网络. E-mail: wind123456@189. cn.

吕琼帅 男, (1985-), 硕士研究生, 讲师. 研究方向为计算机网络、数据挖掘.

赵伟艇 男, (1967-), 硕士研究生, 教授. 研究方向为计算机网络.

(上接第 91 页)

供了一种全新的思路. 系统要求低、安装方便、使用简单、加密效果显著, 可广泛应用于政府、军队、企业等场所.

参考文献:

[1] 李秋华,何为,朱桂斌. 基于 RFID 的磁盘加密系统[J]. 信息网络安全, 2012, 12(9): 27-31.

[2] 刘冰. C++ 程序设计教程: 基于 Visual 2008[M]. 北京: 机械工业出版社, 2009.

[3] 谭文,陈铭聚. Windows 内核安全与驱动开发[M]. 北京: 电子工业出版社, 2015.

[4] 刘荣. 圈圈教你玩转 USB[M]. 北京: 北京航空航天大学出版社, 2009.

[5] John Hyde,孙耀国,赵德刚. USB 设计应用实例[M]. 北京: 中国铁道出版社, 2003.

[6] Jan Axelson. USB 开发大全[M]. 4 版. 北京: 人民邮电出版社, 2011.

[7] 赛普拉斯总部. AN61347-NX2LP-Flex USB to NAND Flash Firmware Design Notes [EB/OL]. [2016-05-08]. [http://www. cypress. com/d-ocumentation/appli-cation-notes/an61347-nx2lp-flex-usb-nand-flash-firm-ware-design-notes](http://www.cypress.com/d-ocumentation/application-notes/an61347-nx2lp-flex-usb-nand-flash-firmware-design-notes).

[8] 赛普拉斯总部. AN64408-Getting Started with NX2LP-Flex? [EB/OL]. [2016-03-08]. <http://www. cypress. com/documentation/Applicat-ion-notes/an64408-getting-started-nx2lp-flex>.

作者简介:

何 为 男, (1977-), 硕士, 讲师. 研究方向为模式识别、信息安全. E-mail: cqchhw@126. com.

于 洋 女, (1991-), 学士. 研究方向为信息安全、无线通信.

晁志超 男, (1982-), 博士, 讲师. 研究方向为图形处理、信息安全.