基于 PNP 自动映射分区的安全 USB 技术研究与实现

陈伟东[1,2],曾 勇[1],张 力[2]
(1.福建伊时代信息科技股份有限公司,北京 100085;
2.清华大学 软件学院,北京 100085)

摘 要:目前多数安全 USB 设备使用时,需要开启一个应用程序界面来对 USB 设备进行读写、加密/解密。对此,提出并实现了一种利用硬件 PNP 技术自动对 USB 映射为本地盘符,拔下时自动删除盘符的技术。读写文件时,对 USB 设备自动透明加解密;安全 U 盘使用前经过授权中心统一注册与授权,划分为权限注册区和加密区;用户密码验证采用基于密码的密码系统说明书(RFC2898)和应用伪随机函数导出密钥(PBKDF2);权限管理采用预先设定好的内、外网策略,内网策略分为多个等级。在实际应用中取得了较好效果。

关键词:移动存储;加解密;卷映射;硬件插拔

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1674-7720(2010)23-0023-03

Research and implementation of USB technology based on PNP automatic mapping local

CHEN Wei Dong[1,2], ZENG Yong[1], ZHANG Li[2]
(1.Fujian Etim Information and Technology Co., Ltd., Beijing 100085, China;
2.Software College, Tsinghua University, Beijing 100085, China)

Abstract: Now most secure USB device need to open an application GUI to read, write, encryption and decryption. This paper implements a proposed use of the USB hardware PNP technology automatically mount the local drive letter, automatically dismount the drive letter when plug off. Read and write files on the USB device automatically transparent encryption and decryption. USB disk must use the security center before the authorized unified registration and licensing, registration area is divided into permissions and encryption area. User password authentication using password-based cryptography manual (RFC2898) and pseudo-random function to export the key application (PBKDF2). Rights management using pre-configured within the network outside the network strategy is divided into multiple levels within the network strategy, in practice achieved better results.

Key words: removable storage; encryption and decryption; mount; PNP

大多数普通安全 U 盘通过使用软件实现安全 U 盘加密功能。在使用过程中,用户需要打开专用的 U 盘浏览器或管理工具等,不但操作不方便,而且不符合 USB 设备使用习惯和人性化设计。

本文通过对驱动层硬件插拔(PNP)的研究,在用户接上 USB 等存储设备时,在卷过滤驱动层判断符合卷格式的 USB 设备时,如果符合规定的卷格式和标识,则对 U 盘自动卷映射(mount)为本地磁盘,对 U 盘的读写操作如同操作本地盘,即在写入文件时自动加密,读文件时自动解密,对卷映射的本地磁盘盘符的读写,实际是对 U 盘上加密数据的读写。

在分析了 Windows DDK/FSD 驱动开发技术、卷上过滤驱动技术,提出了在 Windows 系统插入 USB 设备时,自动挂载符合规定卷格式的 USB 设备,映射为本地磁盘,根据注册信息和本机是否在内网,应用相应的策略,对 USB 设备进行可读、可写、禁用等措施;在加解密方面,应用基于密码的密码系统说明书(RFC2898)和应用伪随机函数导出密钥(PBKDF2)等标准,保证了数据的

安全存储。

1 原理与架构

系统分为驱动层和应用层，驱动层包括一个卷过滤驱动程序和一个文件系统过滤驱动；应用层包括一个应用程序和与驱动交互的dll。应用层是隐藏界面的应用程序。卷过滤驱动对USB盘的(PNP)动作识别，读移动硬盘卷的头为512 B，对特定标识识别，如果不符合卷标示，则可采用禁用或放行等；如果符合卷格式和标识，则对此卷进行映射。USB盘上数据采用透明加解密方法。

普通U盘使用前需要格式化，物理U盘上的数据是随机的数值。密码算法采用基于口令的密码系统(RFC2898)，口令和盐(salt)结合产生密钥。盐可看作是对口令导出的一个大密钥集合的索引。盐和迭代次数构成了PKCS#5v1.5中基于口令加密基础。系统总体架构序列图如图1所示。

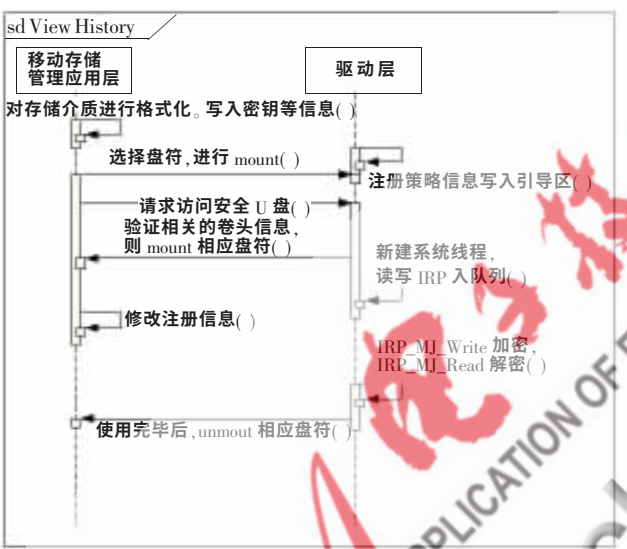

图1 移动存储介质自动mount图

加密算法可采用AES-256、Serpent、Twofish等，解密时通过判断厂商标识以及CRC-32校验和是否正确，在此过程中在权限注册区读入相应的注册信息，如GUID和厂商标识等。如上述过程正确，则执行正确的卷映射过程。

2 研究与实现

系统应用层主要由三个线程组成，主线程是应用程序，剩下卷映射线程和卸下卷(unmount)线程分别用来在USB存储设备做PNP时对本地盘进行卷映射和卸下卷。线程和驱动层采用事件通信机制。本系统定位于移动存储设备，包括移动硬盘、U盘及移动存储卡等移动存储介质。可以将用户的普通USB存储设备分为密文区与权限注册区两个存区。密文区是从内部可信计算机拷贝数据到USB存储设备，数据在后台加密处理后存放的区域；权限注册区则写入GUID和必要的厂商、运行权限、内外网策略等。

卷映射线程收到底层USB的PNP动作时，首先得到运行环境，根据运行环境得到USB存储设备读写权限，然后根据相关密码、密钥等参数通过DEVICEIOCONTROL通知驱动创建本地虚拟盘，最后广播DBT_DEVICEARRIVAL消息通知操作系统。卸下卷线程收到USB存储设备拔出事件通知后，将盘符参数下发到驱动层，对盘符做卸下卷操作，同时清理相关资源，发送广播消息(DBT_DEVICEREMOVEPENDING)消息。

集中注册与授权，使用前必须经过授权中心统一注册与授权，包括格式化、实名注册、标识密级、指定授权计算机、是否采用口令保护等。授权后的移动存储介质在涉密计算机上能正常使用，当未授权的移动存储设备接入计算机时，系统可自动关闭USB端口，使未授权移动存储介质无法在涉密计算机上使用。采用透明加密技术实现读写数据自动加解密。

对于正确安装了移动存储安全系统客户端的计算机，客户端自动上报该机状态，完成到控制台服务器注册功能，有效防止非法用户安装客户端程序。灵活的注册策略，可设定移动存储介质允许的计算机或组；管理员可随时更改移动存储介质注册策略和信息，包括远程策略变更、挂失和注销等；外出拷贝功能是将COPY到U盘内安全存储的数据与外界没有安装客户端程序的计算机进行数据交互使用，非法外联监控；审计功能包括详细审计记录(如注册信息、使用信息和文件操作信息)，记录要素包括使用人、使用的计算机、使用时间和动作等。

应用层完成对移动存储设备的格式化工作。对卷起始位置写入密码、校验和等信息，提供了FAT32和NTFS两种文件系统格式。在驱动中对移动存储设备做卷映射，创建类型为FILE_DEVICE_DISK卷过滤驱动，使用不同的盘符。在IRP_MJ_WRITE和IRP_MJ_READ请求例程中进行加解密。在IRP_MJ_WRITE分发例程中把相关的IRP存入队列。在新创建的系统线程内进行卷加密。在IRP_MJ_READ中进行解密。

注册主要由应用层注册工具完成，可由用户选择FAT32或NTFS格式。注册流程如下：访问移动存储盘，输入需要注册信息。注册信息包括：移动存储盘密码、标签名、安全等级、客户标识名、分区个数、内网移动存储策略、外网移动存储策略、1~5等级的移动存储策略(是否启用保密区、是否启用交换区，不同分区间操作控制)。然后写入移动存储密码和相关注册信息，使用IOCTL向移动存储介质写入相应的控制权限信息。

插入安全U盘后，得到处理环境信息：是否为有效设备、是否有客户端代理、客户标识匹配、在内网否、安全等级是否1~5，然后决定应用不同策略。驱动只要挂载存储卷的UpperFilter即可完成卷的加解密任务。

卷过滤驱动在IRP_MJ_PNP请求时监控设备的插拔

消息，程序判断是否是指定的卷格式，如发现是移动存储设备，则用 DeviceIoControl 与驱动层通信。通过对新加卷的监控，实现对移动存储设备的加解密。应用层通过 DeviceIoControl 与应用层的通信获得用户密钥和权限策略。

在文件系统驱动层映射卷的流程如下：应用程序调用 ZwCreateFile 或 IoCreateFileSpecifyDeviceObjectHint，I/O 管理器确定请求的目标是哪个逻辑卷，检查是否设置了 VPB_MOUNTED。如此卷在系统引导后未被卷映射，则 I/O 管理器发送卷映射请求(IRP_MN_MOUNT_VOLUME)。

每个文件系统接收到卷映射卷请求后，检查卷引导扇区确认是否是正确的卷格式、卷是否为指定的文件系统格式化的。如果卷格式符合，文件系统则卷映射该卷。

对移动存储设备的格式化可分为 FAT32 和 NTFS 两种格式。卷过滤驱动监控系统的 PNP 行为，如移动介质头 512 B 符合卷头格式，则使用事件通知应用层对移动介质卷映射，卷映射线程将相关参数(盘符、密码、磁盘属性)等传递到文件系统驱动，创建一个 FILE_DEVICE_DISK 类型的过滤设备；然后创建一个线程，在线程中应用 ZwCreateFile 打开卷设备 Handle，读取卷头信息，对卷头信息进行验证，如验证卷头信息成功，则创建相应盘符的符号链接；对 USB 设备加密模式为 XTS；卸下卷线程接到拔下 USB 存储器通知事件后，对相应盘符进行卸载，清理相关资源。

应用层包括对卷格式化功能，对移动 USB 设备合法性验证、得到 USB 运行环境信息、根据策略信息对 USB 设备进行读写、禁用等控制。在 USB 设备上单开辟一个区域，用来存取注册信息以及写入注册信息和读取注册信息，生成 GUID 写入 USB 设备的唯一标示，完成卷映射功能。

安全 U 盘总体设计序列图如图 2 所示。

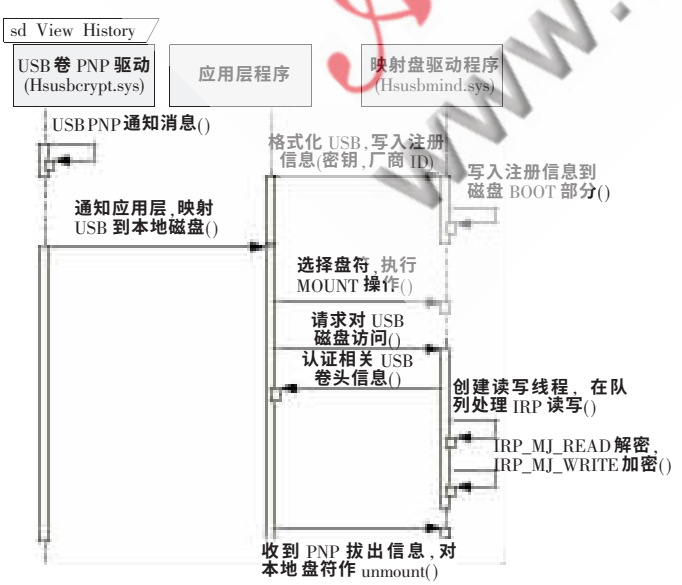

图 2 安全 U 盘总体设计序列图

在 PNP 发生时，驱动层和应用层通过事件进行通信。对卷映射和卸下卷过程各启动一个线程等待 PNP 事件发生。首先验证卷头格式，卷头信息读到 RAM 中。卷头 64 B 是生成密钥所需的盐(salt)，驱动层解密读入的标准卷头、解密过程中的所有数据保存在 RAM 中。在此过程中需要得到如下参数：

卷头导出函数用的 PRF 参数(见 PKCS #5 v2.0)可为：HMAC-SHA-512、HMAC_RIPEMD-160 等；厂商标示密码和读入的盐值传给卷头密钥导出函数，生成头解密密钥和扇区解密密钥；使用的加密算法为 AES-256；解密时对照厂商标示密码及校验和，密钥用来解密卷上的扇区。

主要数据结构和参数如下：

(1)卷映射数据结构

```
typedef  struct
{
Int     nReturnCode;                    //底层 sys 返回码
Short       wszHsVolume[MAX_PATH];          //卷名称
Password    VolumePassword;                 //用户密码
BOOL        bCache;             //是否在驱动中缓存密码
Int         nDosDriveNo;        //需要卷映射的盘符号
Int         BytesPerSector;                 //扇区字节数
BOOL        bSystemVolume;                  //是否为系统卷
BOOL        bPersistenVolume;               //是否为隐藏卷
BOOL        bMountReadOnly;  //是否映射为隐藏卷格式
BOOL        bMountRemovable;        //是否映射为可移动
                                            //存储设备
} MOUNT_STRUCT;
```

(2)设备信息结构

```
typedef  struct  _SECDEVICEINFO
{
CHAR     szProvider[SD_MAX_PROVIDER_LEN];
                                    //设备提供者名称
DWORD    dwDeviceType;                  //设备类型
CHAR     szDeviceID[SD_MAX_DEVICE_ID_LEN];
                                    //设备唯一标识
__int64    dwDeviceCapacity;            //设备容量
} SECDEVICEINFO,  *PSECDEVICEINFO;
```

(3)策略数据结构

```
typedef  struct   _POLICYDATA
{
BOOL     bEnableSecPart;          //是否启动保密区
BOOL     bReadSecPart;            //是否可读保密区
BOOL     bWriteSecPart;           //是否可写保密区
BOOL     bEncryptSecPart;         //是否加密保密区
BOOL     bEnableExchPart;         //是否启用交换区
BOOL     bReadExchPart;           //是否可读交换区
```

```
BOOL    bWriteExchPart;          //是否可写交换区
BOOL    bEncryptExchPart;        //是否加密交换区
BOOL    bExchPartToSecPart;
                    //是否允许从交换区复制到保密区
BOOL    bsechPartToSecPart;
                    //是否允许从保密区复制到交换机
} POLICYDATA, *PPOLICYDATA;
```

应用层创建双线程,等待 PNP 消息,如接入 USB 盘符和特定卷格式,则对卷做相应卷映射和卸下卷。

对卷卷映射函数:

```
Int MountVolume (
                int driveNo,
                char *volumePath,
                Password *password,
                MountOptions *mountOptions,
                BOOL bReportWrongPassword );
```

对卷卸下卷函数:

```
BOOL    UnmountVolume
(int nDosDriveNo, BOOL forceUnmount );
```

创建内存中卷格式:

```
int VolumeWriteHeader (char*header,int ea,int mode,
                Password* password,
                char*masterKey,
                PCRYPTO_INFO*retInfo,
                BOOL bWipeMode );
```

读入 USB 卷头:

```
int VolumeReadHeader(char*encryptedHeader, Password);
```

经过测试人员测试和客户现场应用,本系统达到了良好的应用效果,从驱动层到应用层都运行良好。系统支持 FAT32 和 NTFS 格式,对容量较大的 USB 移动存储设备和容量较小的 U 盘都有较好的使用和保密效果。

参考文献

[1] 胡晓军.开发 WDM 型 USB 设备客户驱动程序[J].中国数据通信,2002(2):51-53.

[2] RUSSINOVICH M E, SOLOMON D A. 深入解析Windows操作系统[M].第 4 版.潘爱民,译.北京:电子工业出版社,2008.

(收稿日期:2010-07-01)

作者简介:

陈伟东,男,1970 年生,高级工程师,主要研究方向:信息系统安全。

曾勇,男,1975 年生,硕士,高级工程师,主要研究方向:网络与系统安全管理。