

基于过滤驱动的局域网透明文件安全加密方法

梅凯珍, 李永忠

(江苏科技大学 计算机科学与工程学院, 江苏 镇江 212003)

摘要:针对企业局域网文件安全问题,文中提出了一个基于过滤驱动的局域网透明文件安全加密方法,阐述了透明加密过程中加密进程获取、加密标志设置以及加密处理关键技术,同时还介绍了加密系统的几个主要功能模块。最后通过使用透明加密技术以及对称加密算法 AES 实现了对文本文档的加密实验,证明了文中提出的过滤驱动技术在实际应用中的可靠性,实现了对局域网内的文件有效的安全管理,加强了局域网文件的安全防护,快捷有效地防止了机密数据内容的泄漏和扩散。

关键词:文件加密;过滤驱动;IRP;局域网

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2012)04-0238-04

Transparent File Safety Encryption Method of Enterprise LAN Based on Filter Driver

MEI Kai-zhen, LI Yong-zhong

(School of Computer Science and Engineering, Jiangsu University
of Science and Technology, Zhenjiang 212003, China)

Abstract: For the security issues of enterprise LAN, propose a LAN transparent file safety encryption method based on filter driver, describing the key technologies of obtaining encryption process, setting encryption flag and dealing with encryption of the transparent encryption process, at the same time introducing some of the encryption system's main modules. Finally, the text of the document experiments using transparent file safety encryption method and AES encryption method show the proposed filter driver technology reliability in practical applications. Then implement effective security management of LAN file. Strengthen the security defense of LAN file and prevent the leakage and diffusion of confidential digital content efficiently and effectively.

Key words: file encryption; filter driver; IRP; LAN

0 引言

在当今社会随着计算机与网络技术的不断发展,企业信息化程度也越来越高,而企业局域网信息安全也成为研究的热点。其中内网信息安全也因其重要性成为众多企业关注的焦点,然而企业很难做到有效控制员工将数据外流泄密的行为,虽然企业对此做出了监控,但是还是防不胜防,在这种情况下可以采取文件加密方式,传统的文件加密方式总会改变用户的操作习惯,并且不能做到强制性加密,局域网透明文件加密由此应运而生。所谓的透明文件加密^[1-3],就是指对用户来说是未知的。当用户打开或编辑指定文件时,系统将自动对未加密的文件进行加密,对已加密的文件自动解密。文件在硬盘上是密文,在内存中是明文。

一旦离开使用环境,由于应用程序无法得到自动解密的服务而无法打开,从而起到保护文件内容的效果。

1 文件过滤驱动原理

目前对于文件加密技术这一领域,主要出现的有微软推出的加密文件系统以及基于钩子(Hook)技术的文件加密技术,但这两种技术也存在缺陷。

下面将详细讨论文件过滤驱动^[4-7]的工作原理。

文件系统驱动主要是负责维护各种文件系统的磁盘结构以及用户与底层非易失型存储介质之间的交互。文件系统驱动工作原理主要是依赖 I/O 管理器的,在文件驱动接收到应用程序 Open、Create、Read、Write 和 Close 文件的请求之前, I/O 管理器要取得文件驱动层在管理器中的注册信息,这样当截取到上层应用程序发送的访问磁盘逻辑卷请求时, I/O 管理器就能够识别这一动作,将请求发送到文件驱动层。当文件系统驱动处理完请求后会将处理完的请求发送到

收稿日期:2011-08-29;修回日期:2011-12-02

作者简介:梅凯珍(1985-),女,湖北黄冈人,硕士生,研究方向为网络安全;李永忠,教授,硕士生导师,计算机应用技术学术带头人,研究方向为网络安全、计算机应用、藏文信息处理。

底层的存储设备驱动程序,通过存储设备驱动程序将文件信息写到物理磁盘上面,如图1所示。

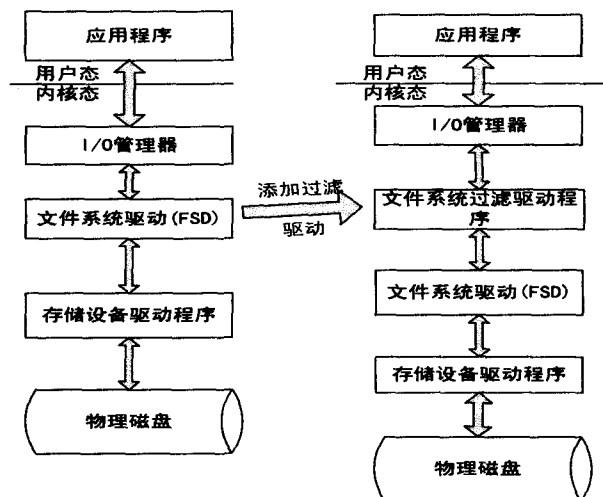


图1 文件系统逻辑结构

由于Windows文件系统的驱动模型WDK (Windows Driver Kit)是采用分层的结构,这样在使用IRP机制的内核层,可以使驱动程序通过将构造的匿名设备对象负载在已知的设备对象上,而这个匿名的设备对象就是所谓的驱动设备对象,与之相关联的驱动程序就是过滤驱动程序。这种分层的结构允许在IRP包到达目标设备对象之前首先会判断有没有匿名的设备对象,如果有就将IRP包发送给匿名设备,匿名设备然后会根据IRP包的信息调用相应的驱动程序处理,当匿名设备加载完成特定的功能之后,然后将IRP包发往下层驱动设备。

2 基于过滤驱动的透明文件安全加密方法

在改进现有的文件安全加密技术的基础上,设计了基于文件过滤驱动的透明文件加密方法,如图2所示。新设计的方法主要分为两大部分:客户端和服务端。客户端模块的主要作用是给终端用户提供客户端

身份认证、透明加密和解密服务、访问控制等服务功能。客户端按操作系统的运行可分为用户态和内核态,用户态主要实现通信代理、策略配置、密钥管理、读/写操作等功能,而内核态主要实现过滤驱动技术也是要讨论的重点,用户态主要是为内核态提供加密服务的;服务端模块的主要作用是方便管理员有效地控制整个加密系统,并为客户端提供策略分配服务,所有的客户端请求都将通过策略服务器得到响应。

过滤驱动关键技术:

为了实现对文件的加解密与访问控制,需要拦截上层发送的包(I/O Request Packet, IRP),如图2所示。当拦截到加密写操作IRP包时,则申请新密钥与文件加密标志,从IRP指定的地址中读取明文,用对称加密算法对其加密,并且向下层传递IRP将密文写入磁盘上,最后在完成方法中恢复明文信息,同时把文件的相关信息记录到文件加密属性中,否则正常处理。

当拦截到读操作IRP包时首先判断当前文件是否存在密钥,如果存在,则解密,否则直接把数据向下提交。

以上分析了加解密的主要流程,下面将对获取机密进程、加密标志设置以及加密处理等关键技术进行研究。

2.1 获取机密进程

在经过加密的操作系统中,所有的进程被分为两类:机密进程和普通进程^[8,9],但是由于进程的名字很容易被伪造,所以在内核中,可以对进程名与同名可执行文件的内容进行验证,来防止非法的仿冒行为。首先获取当前进程的名字,EPROCESS结构是Windows内部的每个进程都维护的一个保存进程名的结构。在内核模块的DriverEntry函数总会执行一个名为"System"的进程,那么可以确定DriverEntry当前进程名为"System"。虽然不知道EPROCESS结构的具体内容,但是可以在EPROCESS中搜索"System"这个字

串,一旦搜索到,记录下偏移位置。这样,以后要从EPROCESS获得进程名字时,就可以直接从这个位置取了。下面介绍具体的伪代码实现。

首先在获取进程名字之前要先进行初始化,初

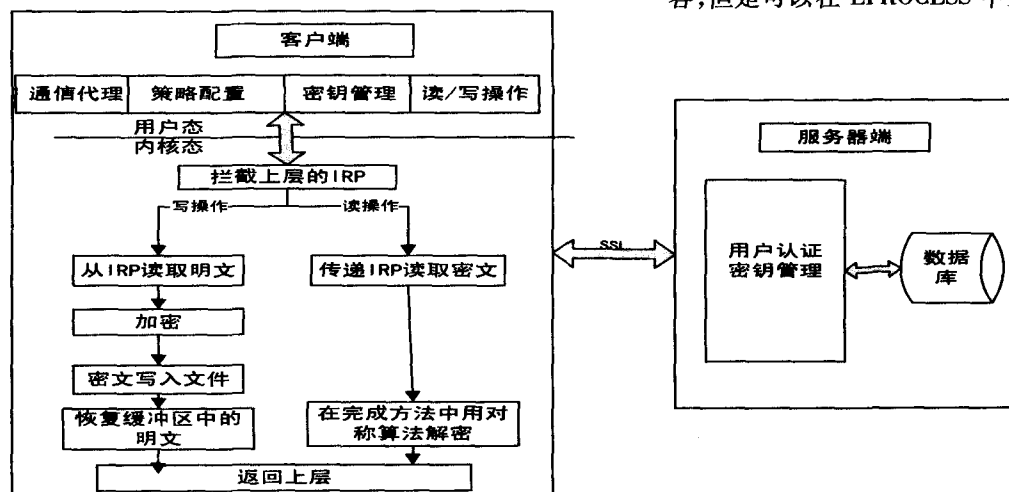


图2 文件加密方法

始化函数为 cfCurProcNameInit,这个函数必须在 Driv-

erEntry 中调用,否则 cfCurProcName 将不起作用。并且设置静态变量 size_t s_cf_proc_name_offset=0;保存要寻找的偏移位置,这个函数很简单。先通过 PsGetCurrentProcess 得到当前 EPROCESS 的位置,然后充分相信其中有一个字符串"System",搜索后得到偏移位置保存在一个静态变量中,下面的 cfCurProName 函数就是获取程序名字的关键代码。

```
ULONG cfCurProName(PUNICODE_STRING name)
{
    EPROCESS curproc;//声明一个 EPROCESS 指针
    ULONG i,need_len;
    if(s_cf_proc_name_offset==0)
        return 0;
    curpro=PsGetCurrentProcess();//获得当前进程,
    然后移动一个偏移位置得到进程名所在的位置
}
```

2.2 加密标志设置

当机密进程获取一个文件时,如何判断这个文件是已经加密的还是未加密的,这需要在硬盘中保留一个文件是否已经被加密的信息,这种信息称为加密标志。这种信息必须保存在硬盘上,和文件一起存在。一个选择是,在文件以外的地方保存这个信息。比如另建一个隐藏文件,保存当前目录下其他文件的加密标志,但是这种方法非常麻烦,所以在此选择在文件内容中保存加密标志,在文件内容中保存加密标志也有两种选择:基于文件头和文件尾,基于文件尾比较容易实现但是有安全隐患,在此选择基于文件头,选择文件头的好处是稳固可靠,位置固定缺点是实现起来相对要困难。由于要实现对所有的机密进程隐藏这个头部,则所有文件都要增加一个偏移,下面给出了一个记事本隐藏文件头的设置偏移,比如记事本如果试图把文件大小设置为 1kB,假设文件头为 4kB 大小,那么实际的文件应该被设置为 5kB,实现的伪代码如下:

//对所有设置请求进行修改,使之隐去前面的 4kB 文件头

```
Void cflrpSetInforPre (PIRP irp, PIO_STACK_LOCATION irpsp) {
    PUCCHAR buffer = irp -> AssociatedIrp. System-
    Buffer;//取得文件缓冲句柄
    NTSTATUS status;
    ASSERT(irp->MajorFUNCTION==IRP_MJ_SET_
    INFORMATION);//用于调试环境的声明
    switch(irpsp->Parameters. SetFile. FileInformation-
    Class)
    {
        case FileAllocationInformation: {
```

```
.....//增加在 FileAlloca-
tionInformation 条件下的文件偏移
    }
    .....};
}
```

上面只给出了 FileAllocationInformation 一种情况,其他情况类似,通过隐藏文件头,就可以在文件头设置加密标志。

2.3 加密处理

当上层的应用程序对某一类文件设置加密操作的规则,底层的过滤驱动层截取到文件创建的 IRP 请求时,则首先读取文件加密标志,根据加密标志来决定是否要进行加密操作,如果需要进行加密操作,则通过事先写好的加密函数一般使用 AES 加密算法,从服务器获取加密密钥对文件进行加密。当加密好文件之后根据写 IRP 请求将加密好的文件写入物理磁盘。

当对加密过的文件进行读请求时,首先判断是否可以通过 FastIODispatch 例程在 Cache 管理器处获取。如果可以的话直接从 Cache 中读取明文,否则调用底层驱动从磁盘读取数据,在应用层获得服务器的解密密钥通过 I/O 完成例程对文件数据进行解密操作^[10-12]。下面的代码主要针对文件的加密操作:

```
NTSTATUS EFWrite (IN PDEVICE_OBJECT DeviceObject,IN PIRP Irp) {
    .....
    if (IS_Control_MY_DEVICE_OBJECT( DeviceOb-
    ject)) {
        .....
        CompletionIoRequest ( Irp, IO _ NO _ INCRE-
        MENT);//完成不需要加密的请求
        return STATUS_IRP_INVALID_DEVICE_RE-
        QUEST;
    }
    IoCopyCurrentFileToNextIrpStackLocation ( Irp );//
    拷贝需要写入文件的数据到新开辟的 MDL 内存
    EncryptMyFile( dataBuffer,length,key );//加密函数
    的调用
    }
    解密操作类似,在此就不做赘述。
```

3 实验与结果分析

建立测试环境如下:acer 台式机一台,CPU 为 Pentium(R) Dual-Core E5300 2.60GHz,内存为 2G,硬盘 250G,操作系统为 Windows XP(SP2)。

通过配置了 TXT 文档的文件保护策略并使用了 AES 对称加密算法,在一个既有 FAT 分区也有 NTFS

格式分区的操作系统中,进行文件的操作,结果表明系统可以在 FAT 分区和 NTFS 分区很好的工作,对所有 txt 类型文件都进行了加密存储,写入的明文如图 3 所示。

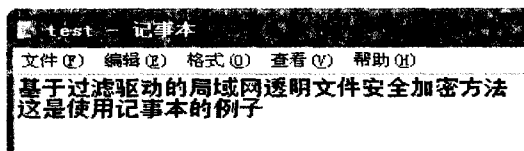


图3 文件保存的明文

当在另外一台没有加密方法的电脑上看这些文件都是乱码,看不到真实信息,如图 4 所示:

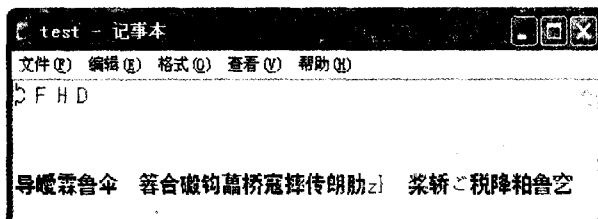


图4 文件实际存储的密文

并且还对加密过程使用 DebugView 进行了检测,通过使用 DebugView 的检测可以对内核态程序的运行过程有一个大致的了解,如图 5 所示:

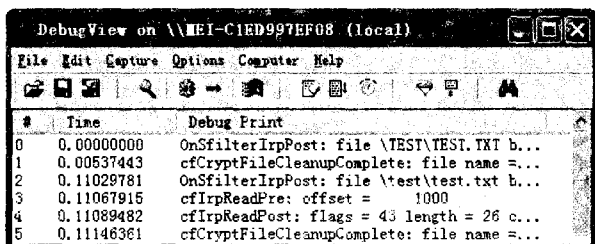


图5 文件加密过程

实验结果表明基于过滤驱动的文件加密方法可以在不改变用户的使用习惯的情况下很好地提供加密与解密操作。

4 结束语

利用文件系统过滤驱动技术进行文件透明加密和解密是一种在 Windows 内核里实现的底层开发技术,

开发实施起来相对较繁琐,但是它可以在不改变用户的习惯的情况下有效保护局域网内各种电子文件信息安全,在安全性方面也有了很大改善,具有较高的商业价值和较好的社会效益。

文中实现的局域网文件加密技术对局域网内部的信息安全有一定的保障,但是还有许多需要完善的地方。

参考文献:

- [1] Sun Qindong, Guan Xiaohong, Zhou Yadong. A Survey of Network Information Content Audit[J]. Journal of Computer Research and Development, 2009, 46(8): 1241-1250.
- [2] Zhao Mingwei, Mao Rui, Jiang Rongan. Transparent Encryption File System Model Based on Filter Driver[J]. Computer Engineering, 2009, 35(1): 150-152.
- [3] Shen Wei, Wang Lei, Chen Jiajie. Design and Implementation of Encryption System Based on File System Filtering Drive[J]. Computer Engineering, 2009, 35(20): 157-159.
- [4] Liu Haiyan, Yang Zhaohong, Huo Jinghe. On the Detection and Analysis Techniques of the Intranet Security[J]. Computer Engineering & Science, 2009, 31(9): 11-12.
- [5] 胡宏银,姚峰,何成万.一种基于文件过滤驱动的 Windows 文件安全保护方案[J]. 计算机应用, 2009, 29(1): 168-171.
- [6] 王全民,周清,刘宇明,等.文件透明加密技术研究[J]. 计算机技术与发展, 2010, 20(3): 147-150.
- [7] 吴慧玲,贺广生.一种基于系统驱动的文件透明加密系统的实现[J]. 计算机与现代化, 2010, 5(4): 156-158.
- [8] 顾正义,黄皓.新加密文件系统的研究与实现[J]. 计算机工程与设计, 2009, 30(4): 3271-3277.
- [9] 赵晓峰,叶振.几种数据库加密方法的研究与比较[J]. 计算机技术与发展, 2007, 17(2): 219-223.
- [10] 徐翔.文件保护系统中透明加解密技术的设计与实现[D]. 北京:北京化工大学, 2009.
- [11] 李民.基于 Windows 文件系统过滤驱动的文件加/解密技术研究与实现[D]. 成都:四川大学, 2006.
- [12] 谭文,杨潇,邵坚磊.寒江独钓-Windows 内核安全编程[M]. 北京:电子工业出版社, 2009.

(上接第 237 页)

4243-4248.

- [9] Castagnos G. An efficient probabilistic public-key cryptosystem over quadratic fields quotients[J]. Finite Fields and Their Applications, 2007, 13(3): 563-576.
- [10] 汪祥莉,李腊元,王文波.一种基于网络安全的复合加密算法的研究[J]. 武汉理工大学学报, 2008, 32(5): 845-848.

- [11] Bao Feng, Lee Chengchi, Hwang Min-Shiang. Cryptanalysis and improvement on batch verifying multiple RSA digital signature[J]. Applied Mathematics and Computation, 2006, 172(2): 1195-1200.
- [12] 佟晓筠,姜伟.基于混合加密技术的电子商务安全体系研究[J]. 微处理机, 2006, 4(2): 45-47.