基于Windows文件系统访问控制技术的研究

靳书超
中国人民大学　北京　100872

摘　要：文章在分析了常用的文件控制存取方式后，指出了从下层进行限制的优越性。接着详细分析了视窗系统的内部工作机理，揭示了视窗系统中用户层与内核层之间的协同工作，并对其各组成部分的功能进行了详细的分析，重点讨论了在底层实现文件存取控制的技术。最后，结合作者自己的一个例子，对实际的控制过程进行了说明。

关键词：Windows；文件系统；访问控制

Research on access control technology based on Windows File System

Shuchao Jin
Renmin University of China ,Beijing 100872

Abstract: after analyzing the commonly used file control access methods, this paper points out the advantages of restricting from the lower level. Then, the internal working mechanism of windows system is analyzed in detail, and the cooperative work between user layer and kernel layer in Windows system is revealed. The functions of its components are analyzed in detail, with emphasis on the technology of realizing file access control at the bottom. Finally, the actual control process is illustrated with an example of the author.

Keywords: windows, file system, access control

前言：

Windows操作系统由于使用简便、操作简单，占据了大多数用户的大多数，但在使用便利的同时，也让广大用户感到了一系列问题。例如：似乎对病毒的侵入和毁坏束手无策。经常需要其他的软件来保护自己。这导致了Windows的CPU时间浪费，并且系统的运行速度也显著降低。最近几年，电脑失窃、重要资料失窃的案件不断发生，让很多人心惊胆战。事实上，很容易就能发现，这些问题的根源在于未经许可的使用者的违法行为。因此，本文对Windows文件系统的存取控制作了初步的探讨。Windows系统的整体设计采用了分层的设计思想。核心架构界面为使用者架构的应用程式提供服务。在核心模式下，每个模块都有自己的任务，并有一个很好的机制，可以确保每个模块之间的通讯正常，经过一层又一层的调用，最后，从用户层面上完成了请求的操作[1]。事实上，整个视窗系统就是一个巨大的社会管理系统：使用者只有在接待处才能处理自己的需求。而前台只会把你的请求转交给主管，再由主管转交给主管部门。看似是前台的工作人员帮你处理，但实际上，你的要求是一层一层的传递，最后有一个人来处理，这就是你的要求。然后，我会将你的要求，传递到你的脑海中。作为使用者，您只能与前台的工作人员进行交流，您将无法看到幕后的操作。

一、系统访问控制技术

由于办公自动化的不断发展，人们把自己的重要文件资料储存在电脑上，代替了传统的纸质文件，电脑也被广泛地装备在党政机关、军队等要害单位，各种机密资料被送到电脑上，进行处理、储存、传输。为确保保密资料不被盗用；篡改，非法复制，越权访问，大量的网络安全设施与机制被设计，但是他们忽略了电脑放在桌面上的安全问题，因为黑客可以以合法的身份登陆电脑，越权访问，并且可以肆无忌惮地复制任何所需的机

作者简介：靳书超，1994年9月15日，男，汉族，陕西安康，本科，职称：驱动开发工程师，现主要从事的工作：BSP驱动开发。

密资料。根据CERT的数据，70%以上的电脑犯罪都是由于局内人员使用非法终端进行的，因此，要确保这些数据的安全，除了要阻止黑客入侵外，还要防止非法使用者利用合法的身份登陆，进行非法的操作，盗取或破坏保密文件[2]。当前，对档案数据的存取保护主要采用三种技术：

ACL存取控制技术，HOOK技术，以及文件系统过滤驱动技术，这些技术包括：

1.ACL存取控制技术：根据使用者和群组的概念，将使用者与档案的存取控制清单（ACL）相联系，从而获得存取的权利，这是一种技术，尽管从使用者的观点来说，可以避免别人存取他们的资料，而且，这种技术很难阻止以一个使用者的名义进行恶意程式的存取，而且这种技术只能在NTFS档案系统中使用。

2.HOOK技术：利用Windows提供的API和文件操作触发的视窗信息进行HOOK，并在适当的处理下实现对文件存取的保护。

3.文件系统过滤驱动技术：在文件系统驱动器上装载过滤器驱动器，可以拦截IRP中的全部文件存取请求，并按照特定的存取保护策略来截取对应的IRP，使其在细粒度层次上进行文件的操作，使文件存取得到有效的保护。文件系统过滤驱动是一种核心状态的中间层驱动，它无需更改底层驱动和用户程序，添加新的功能，安全性高，透明度高；具有良好的扩展能力和较好的自我保护能力。本文从三种不同的文件存取保护技术中得到的结果来看，文件系统过滤驱动技术在文件存取保护中的优越性和更强的安全性[3]。

二、种基于过滤的文档驱动技术

这一部分从定义文件系统过滤器驱动和过滤器驱动的工作过程开始，并对其工作过程进行了详细的阐述。

2.1 File System的驱动程序如何工作

文件系统过滤驱动是一种特殊的驱动方式，即将自身装载到视窗NT文件系统驱动程序上，并拦截对基础驱动装置的要求；该系统具有可伸缩性，文件系统过滤器驱动程序可以使用I/O请求的初始目标驱动程序，也可以使用其它的用户服务或核心架构软件来实现新的功能。在向目标装置对象发出文件动作要求之前，I/O管理员会检查在目标装置上面是否安装了额外的装置物体，如果存在，首先将IRP传送到另外的装置，然后通过附加装置的驱动进行处理，然后再传送到目标装置。因此，附加装置物件被文件系统筛选驱动程式建立于档案系统的储存装置之上，执行预定的处理传送至目标装置的作业要求，以控制档案存取，保护档案安全性等。

三、目标管理器

Windows操作系统所提供的服务基本上都是作为一个对象。Windows中有许多被称为“对象”的数据结构。程序员可以读取和写入数据结构中的某些变量，而其他的则需要使用Windows提供的程序。物件管理程序是建立、管理、再利用物件的元件[4]。在驱动开发中，有许多对象，例如Driver Object，Device Object等。

3.1过程管理员

流程管理员负责处理序的建立与结束，而执行绪的排程则由核心来完成。处理序管理程式依赖于其它的执行程式元件，例如物件管理程式、虚拟记忆体管理程式等等。

3.2虚拟记忆体管理员

虚拟存储器与实体存储器的概念不同。在CPU的MMU（MMU）的帮助下，物理记忆体与虚拟记忆体之间存在着一定的关系。虚拟存储器管理员是一个负责管理虚拟存储器的软件。当申请、回收虚拟内存等操作时，通过这个模块来完成。

3.3输入输出管理程序

I/O管理程序负责启动I/O的请求，并对其进行管理。它包含了一系列的核心模式的程序。这些程序提供了在用户模式下处理序的统一界面。不管是读写端口，访问键盘，或磁盘文件。所有的动作都是以IRP的请求格式来实现的。在IRP中，IRP包括了一些关键的数据，比如读操作或写操作，读多少个字节，写多少个字节。IRP被传输给特定的驱动，由它来执行IRP，把已完成的状态回到用户模式[5]。在实践中，I/O充当了使用者程式码与装置驱动程式的介面。

3.4对管理员进行配置

在windows上，配置管理器会记录电脑的全部软件和硬件配置。它用一个叫做登记中心的数据库来存储数据。设备驱动程式会依照登记资料载入。此外，该驱动还能从注册中心抽取相关的参数，从而增强了驱动的灵活性。比如，一个装置的运行延迟，可以被写入到一个登记中心中。当你写程式时，驱动程式会读取这个数值，而非写入一个固定的数值。

3.5驱动器

I/O管理器接收到一个应用程序的请求，就会建立对应的IRP，然后把IRP发送给驱动来进行处理。

（1）直接按照IRP要求对特定的硬件进行操作，然后再执行该RP，再返回。

（2）向基础驱动发送这个IRP请求，然后等待基础驱动的返回。

（3）收到IRP要求后，不要急着处理。而是将新IRP分配给其它的驱动，然后等待它的反馈。以下是关于档案系统的论述。

Windows的设计者为了简化对不同的设备的操作，使其能够对各种设备进行统一的界面，并把它们看成是一个正常的文档。这意味着，在windows里，不管是什么设备，都是用来运行文件的。当然，更别提在磁盘上的档案了。所有的档案都储存在一个磁碟里，当使用者提出档案要求时，档案系统会产生对应的1个RP，然后把IRP传送到磁碟驱动器，磁碟驱动器会特定地存取磁碟，并把存取的结果一层一层地传送到使用者。Windows上常用的两个文件系统是FA32和NTFS，它们的驱动是fastfat.sys和ntfs.sys。可见，要想存取档案，必须要有档案系统的驱动，如果我们能够加入一定的限制程式，就可以控制档案存取。实际上，我们有机会在IRP下传的每个阶段进行限制。

以下就是我自己写的一个实例，我们可以从这个例子中了解到驱动程序的思想和实现文件存取的方法。在特定的实施中，有两个模块，一个是应用，一个是驱动。在这个应用程式里，使用者可以选取要保护的档案，并把档案路径储存到登记处。这里存储的是一个注册中心，而不是一个普通的文件，因为每个人都可以使用，可以随时更改。将其放到注册中心中，大多数人都不会注意到。当然，不能有过多的档案路径。而在内核的文件驱动中，我们在启动时，会直接读入登录，然后把所有的文件路径名称都读到一个双向链表中。在此基础上，从应用程序层面上的IRP可以判定文件的路径，如果这个字串出现在链表中，则表示这个档案是一个机密档案，使用者无法存取。此时，在此处直接调用Lo Complete Request功能来完成该请求。因此，从订阅层发出的IRP请求被切断，不再向下传送，而底层没有接收到IRP，因此无法存取任何文件。这样就可以实现对文件的拒绝。当然，如果没有对应的字串，则表示这个档案不是机密档案，应当被存取。那么，就把IRPF发送给真正的文件驱动[6]。

让我们来看看这个驱动，这个驱动是通过一个文件系统，例如fastfat.sys，或者ntfs.sys。而我们的驱动程序，只是简单的筛选，就是让我们觉得不重要的文件进入，而那些敏感的要求，则会被拒绝。这种驱动程序叫做过滤器。当然，驱动过滤器装置必须与实际的档案系统驱动装置相连接（纵向增加）。真正的存取仍然是通过这个驱动的操作系统来实现的，我们只要把我们自己编写的过滤器驱动添加到这个驱动程序中就可以了。让我们一起来看看整个的情况。在用户级程序中，用户可以通过用户选择的方式来筛选敏感的文档，同时，通过对用户的选择，实现对文档的访问控制。以下是主要技术部分的代码。应用：使用Reg Create Key Ex功能，产生一个特定的子关键字，并可以通过它的参数Lpdw Dispition来看到这个子密钥之前有没有。如果有，您需要重新设置一个子键名，您必须确保它不会与已经存在于登录中心的子键名发生冲突。一旦成功，在循环中调用Reg Delete Key功能，就可以向注册中心写入所选择的文件路径。这样，该应用程序的函数就完成了。

驱动：微软的Filter的驱动只是提供了一个能够真正满足它自己设置的过滤需求的框架。这就是我写文件筛选驱动的想法。

在DriverEntW的输入功能中，使用Zw Open Key功能开启注册中心，并对Zw Query Key进行2次调用，每次检测长度，一次进行实际的数据采集。接下来，将Zw Enumerate Key函数进行两次调用，一次获得数据的长度，一次获得（存在于结构中的）真实的文件路径，并将其存储在一个双向链表中。在SfRead功能中，增加了一个循环验证代码：

While（…）

if（L一>数据==filenameffomuser）break；

L=L->next；

若存在的话：LoCompleteRequest（PORP，IO_NO_INCREMENT）；

若不存在的：IoSkipCurrentIrpStackLocation（PIRP）；

IOCallDriver（pobject，pirp）；

以上是一个简单的过滤驱动编写过程，采用多种方法，包括常规的破解软件，均无法打开限定的文件，有效的达到了文件保护的目的。

四、基于文件系统过滤驱动的访问控制系统设计

考虑到文件系统的过滤驱动，高的安全性，高的透明性；在此基础上，本文提出了一种新的文件访问控制系统，它具有良好的可扩展性和良好的自我防护能力，在此基础上，提出了一种文件访问控制系统，它是一种以文件系统为基础的文件访问控制系统，它是一种新型的文件访问控制系统，它是一种新型的文件访问控制系统[7]。以下是对该系统各个模块的功能的说明：

1.使用者识别模组

本模块的主要作用是判断目前登录的用户是系统的管理员或一般的用户。

2.文件存取权限设置模块

此模块的主要作用是：对所有的文件进行截取；IRP请求的写入、删除等操作，并且按照上级管理所传送的当前使用者与使用者的档案存取控制规则，包含IRP的直接传送及失败的IRP要求。该系统以文件系统过滤驱动为基础，不依赖于特定的应用程序，解决了ACL和HOOK两种技术在文件存取保护中的不足，可以在用户存取文件的过程中，按照用户的权限和相应的文件的权限，从系统的底层开始。在粒度级上进行文件存取控制是保证最终文件数据安全的关键。

3.通讯驱动组件

它的主要作用是向档案系统过滤驱动器发送当前的用户标识和相应的档案存取控制规则。

4.滤芯驱动装载组件

本模块的主要功能是把档案系统的过滤驱动装入到档案系统的驱动中。

5.档案存取控制单元

此模块的主要作用是：对所有的文件进行截取；IRP请求的写入、删除等操作，并且按照上级管理所传送的当前使用者与使用者的档案存取控制规则，包含IRP的直接传送及失败的IRP要求。该系统以文件系统过滤驱动为基础，不依赖于特定的应用程序，解决了ACL和HOOK两种技术在文件存取保护中的不足，可以在用户存取文件的过程中，按照用户的权限和相应的文件的权限，从系统的底层开始。在粒度级上进行文件存取控制是保证最终文件数据安全的关键。

五、结语

在对当前存取控制技术进行分析的基础上，对其进行了深入的研究，并对其进行了深入的研究。在未来的工作中，我们将继续深入地探讨预防IRP重入和驱动运行稳定性问题。

参考文献：

[1]郭超.基于微服务的企业存储系统的访问控制与上传优化研究[D].华南理工大学，2019.

[2]蒋志强.电子文件安全管理系统的设计与实现[D].兰州交通大学，2017.

[3]杨琼，王冬.一种面向多级安全的文件系统实现机制[J].航空计算技术，2017，47（03）：94-97.

[4]袁艺.强制访问控制技术的研究及在某RTOS上的应用[D].电子科技大学，2017.

[5]林海南，许国春，朱建涛.基于eCryptfs的分级加密文件系统[J].计算机工程与设计，2016，37（12）：3171-3174+3190.

[6]雷林.基于嵌入式Linux的系统完整性认证技术研究与实现[D].电子科技大学，2016.

[7]高斌，翟江涛，薛朋骏.一种VxWorks文件系统层访问控制方法[J].江苏科技大学学报（自然科学版），2015，29（05）：462-466.