文章编号:1007 - 2985(2011)04 - 0046 - 04

# 基于过滤驱动的图书馆网络系统安全监控*

侯春明[1],王 灵[2]

(1. 吉首大学信息科学与工程学院,湖南 吉首 416000;2. 吉首大学图书馆,湖南 吉首 416000)

摘 要:讨论了高校图书馆网络系统安全的现状,介绍了网络过滤驱动的基本原理. 在 Windows 操作系统中,设计了符合 WDM 模型的网络过滤驱动程序,挂载在 TDI 接口上,实现了对网络数据的过滤,此技术的实现对高校图书馆提高网络系统安全有广泛的应用价值.

关键词:过滤驱动,TDI,网络安全

中图分类号:TP393 文献标志码:A

## 1 高校图书馆网络系统安全现状

高校数字图书馆是高等院校的信息资源中心,是为高校教学和科研提供文献信息保障的公共服务系统,对高校教师和学生的教学,科研与学习起着重要的推进作用[1]. 随着计算机网络在高校图书馆中的广泛应用,高校数字图书馆在网络信息安全领域受到的挑战也越来越多. 由于当前广泛应用的 TCP/IP 协议是在可信环境下为网络互连而设计的协议体系,加上层出不穷的黑客攻击以及不断翻新的木马和病毒的干扰,使得高校图书馆的网络环节存在很多不安全的因素,如口令猜测、地址欺骗、TCP 端口盗用、对域名系统的破坏、利用 Web 攻击数据库、邮件炸弹、木马攻击、僵尸网络、内部信息的非法窃取等各种安全问题,这对高校数字图书馆构成了严重威胁. 仅以病毒为例,据金山软件有限公司有限公司统计,2008 年上半年共截获新增病毒木马 1 242 244 个,较 2007 年全年病毒、木马总数增长了 338%,其总数已经超过了近 5 年的病毒数量总和. 而全国有 22 367 994 台计算机感染病毒,与 2007 年比增长了 194%,给计算机用户带来了巨大的经济损失[2].

随着高等院校图书馆的快速发展,网络服务在图书馆信息传播的过程中占据了越来越重要的位置. 随着网络在图书馆中的广泛应用,各种各样的网络攻击行为和非法入侵行为日趋严重. 作为图书馆网络安全的重要应用,网络访问控制变得日趋重要. 在当前高校图书馆主要采用了 Windows 操作系统,在 Windows 操作系统中实现数据包拦截的方式主要有 2 种:用户态下的网络数据包的拦截和利用驱动程序对网络数据包的拦截. 由于用户态下拦截数据包必须在 Winsock 层中进行,无法处理网络协议栈中的底层协议的数据包. 因此很多木马和病毒以及黑客入侵软件都采用了驱动技术进入内核层,可以轻松的避开应用层的网络数据包拦截. 因此,基于网络过滤驱动的网络数据包拦截技术成为保护高校图书馆网络安全的新兴技术,基于过滤驱动技术的网络安全是现代数字图书馆建设中的新兴热点研究领域.

## 2 网络过滤驱动技术原理

由于当前国内的图书馆网络管理系统的运行平台主要是 Windows 操作系统,将重点讨论在 Windows 平台下的网络驱动过滤模型. Windows 驱动采用了分层驱动的 WDM 模型,WDM 模型采用了如图 1 的层次结构,图中左边是驱动的设备对象组成的堆栈. 设备对象是 WDM 为帮助内核程序管理硬件而创

* 收稿日期:2011 - 05 - 26

基金项目:吉首大学校级科研课题资助项目(09JD015)

作者简介:侯春明(1979 -),男,湖南桑植人,吉首大学信息科学与工程学院讲师,硕士,主要从事计算机应用与信息安全研究.

建的数据结构，1 个物理硬件可以有多个这样的数据结构. 处于堆栈最底层的设备对象为物理设备对象 PDO(Physical Device Object). 在设备对象堆栈的中间某处有 1 个对象称为功能设备对象 FDO (Functional Device Object)，在 FDO 的上面和下面还会有一些过滤器设备对象(Filter Device Object). 位于 FDO 上面的过滤器设备对象称为上层过滤器，位于 FDO 下面(但仍在 PDO 之上)的过滤器设备对象称为下层过滤器[3]. WDM 结构分层驱动结构，使得过滤驱动可以互相嵌套，层层叠加. 作为 1 个过滤驱动程序，可以将上层驱动程传进来的 IRP 进行拦截，过滤 IRP，然后进行进一步的处理[4].

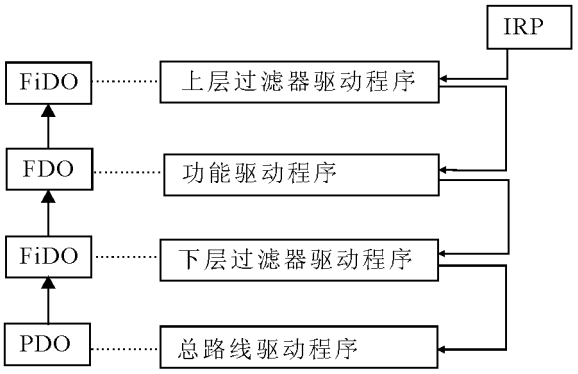


图 1　WDM 中设备对象和驱动程序的层次结构

当前常见的网络应用软件，主要是采用 Socket 编程来实现，Socket 指定以 TCP 或 UDP 方式在传输层进行用户数据的传输. 传输层的数据继续向下层传递，最终在物理层进行信息的传递. 由于应用层的网络应用软件主要采用 Socket 进行网络通信，则应用层的 API 函数如 create 生成 socket 时，将通过 TDI 接口(Transport Driver Interface)达到 NDIS 协议驱动. 由于在网络通信过程中，协议驱动会生成设备，则可以开发基于网络过滤驱动的内核程序，在内核程序中生成过滤设备，将其绑定在协议驱动生成的设备上. 如果某个来自应用层的应用程序要建立连接、打开端口等行为，对应的请求在传递到底层硬件驱动(如网卡驱动)前，都会被过滤驱动捕获，从而对拦截的请求进行判断，如果为合法的请求，继续执行；如果非法，进行拦截.

在网络过滤驱动程序中，要对 TCP/UDP 数据包进行有效的过滤，必须在传输层进行数据包的拦截，这一过程采用 TDI 过滤驱动来实现，TDI 是传输层驱动程序和其他内核模式网络客户的内核接口[5]. Windows 操作系统采用仿真模块支持各种网络接口，比如网络应用软件常用的 socket 就是调用 socket 仿真动态链接库，进而调用 socket 仿真内核驱动程序，然后通过 TDI 与下层的 NDIS 接口进行通信. 因此，各个仿真模块会根据功能的不同，对上层提供网络接口，并将上层的调用匹配成 TDI 调用传递给 TDI 驱动程序. 因此，可以对 TDI 驱动程序进行过滤，进而实现对 TCP/UDP 和 NetBIOS 协议进行各种拦截，从而达到对网络系统安全监控的目的.

## 3　图书馆网络安全的设计与实现

在图书馆的网络安全应用中，图书馆的服务器会经常接收到外部的应用程序的连接请求. 如果设计一个 TDI 层的网络过滤驱动程序，该驱动程序在 WDM 中的设备栈中接近应用层，各种来自应用层的网络应用软件的行为都可以捕获并过滤. 比如当一个连接的建立请求发送到 TDI 层，网络过滤驱动程序能获取对应的连接的进程号、IP 地址等相关信息，判断出打开对应连接的应用程序，进而分析是否为合法的用户和数据等.

在 WMD 模型的 Windows 内核系统中，为 TDI 提供接口的 Windows 协议驱动将在设备栈中生成 TDI 设备[6]. 对于图书馆网络系统安全监控相关的常用协议驱动有“\Device\TCP”和“Device\UDP”，分别为 TCP 协议和 UDP 协议在设备栈中的实现. 网络过滤驱动程序的实现，就是开发一个内核程序，利用 Windows 内核分层驱动的特点，在程序中生成特定的设备，将其在设备栈中绑定 TDI 接口中对应的网络协议的设备，当应用层的各种网络操作以 IRP 的形式传递到下层驱动的过程中，能被过滤驱动捕获，进而根据图书馆网络系统安全监控的各种控制策略做出相应的判断操作.

### 3.1 网络过滤驱动的生成与设备绑定

(1) 驱动程序中创建 DriverEntry 例程. DriverEntry 例程完成对驱动程序的初始化操作，当驱动程序被系统进程所调用并加载到内核中的时候，系统进程将会启动新的线程，调用执行体组件中的对象管理器，创建一个 DRVIER_OBJECT 结构体类型的驱动对象，并将该对象的指针传入 DriverEntry 例程.

(2) DriverEntry 例程的派遣函数进行相关处理. 网络过滤驱动作为 WDM 中的一个驱动挂载到设备链之中后,主要功能是捕获来自应用层传递来的 IPR 信息. 可以在 DriverObject 的指针数组 MajorFunction 中设置相应的派遣函数:pDriverObject->MajorFunction[i] = Dispatch;然后在派遣函数 Dispatch 中,可以根据上层传递的 IRP 的种类的不同,做不同的处理. 对应 TDI 过滤的设计,应该从图书馆网络系统安全监控的实际出发,过滤需要的一部分请求信息,而绝大部分与网络系统安全监控无关的请求应该直接传递到下层设备中,以保障 Windows 操作系统内核的正常运行. 可以通过内核函数 IoSkipCurrentIrpStackLocation 和 IoCallDriver 来实现上层驱动传来的 IPR 穿过过滤驱动传递到下层驱动程序.

(3) 实现挂载. 过滤驱动程序的挂载. 需要在网络过滤驱动中创建一个新的隶属于本层驱动对象 DriverObject 的设备对象,该设备对象用指针变量 pnDeviceObject 来指向 DriverObject:

```
NTSTATUS status = IoCreateDevice(pDriverObject,0,&name,0,0,FALSE,&pnDeviceObject);
```

(4) 将过滤驱动中创建的设备对象挂载到驱动设备链中. 将网络过滤驱动中创建的设备对象挂载到 TDI 接口中各个网络协议所对应的控制设备上,如对 TCP 协议对应的 TDI 控制设备的挂载可以采用内核函数 IoAttachDevice 来实现:

```
RtInitUnicodeString(&devicename,L"\\Device\\Tcp");
IoAttachDevice(pnDeviceObject,&devicename,tcpoldobj);
```

3.2 在网络过滤驱动中实现数据的过滤

利用网络过滤驱动可以实现很多功能,在图书馆网络系统安全监控的应用中,最关注应用层连接请求的 IP 地址和端口以及对各种网络数据的分析判断. 按照图书馆网络的安全策略,进而针对不同的情况进行各种处理. 比如,在高校图书馆的网络访问中,如果某台计算机受到特定的病毒感染,可能对图书馆网络服务器发送大量的数据包进行攻击. 确定了对应计算机的 IP 地址后,可以在网络过滤驱动中捕获到对应的连接请求后,对其进行拒绝.

3.2.1 在网络过滤驱动获取 IP 地址和端口 在网络驱动中,要接收到大量的各种 IRP 请求,当应用层的软件产生了连接请求,一般通过 API 函数 ZwCreateFile 的调用来引发生成请求,对应的 IRP 主功能号为 IRP_MJ_CREATE. 在网络过滤驱动的设计中,可以在 IRP_MJ_CREATE 的派遣函数中对生成请求的 IP 地址和端口进行判断. 当 ZwCreateFile 函数的调用产生的时候,会将 FILE_FULL_EA_INFORMATION 类型的数据传递给底层驱动,在网络过滤驱动程序中捕获到对应的 EA 数据后,可以利用内核中的宏 TdiTransportAddress 和 TdiConnectionContext 来获取传输层的 IP 地址和对应的连接的端口.

3.2.2 对网络数据的过滤 在图书馆的网络系统安全监控的应用中,重点是监控各种通信的数据是否符合图书馆网络通信的要求. 在传输层中,广泛应用的数据传输形式为流式传输和报式传输,其对应的网络协议分别为 TCP 和 UDP. 在网络过滤驱动程序中,可以在主功能号为 IRP_MJ_INTERNAL_DEVICE_CONTROL,次功能号为 TDI_SEND 和 TDI_RECEIVE 的 IRP 所对应的派遣函数中实现流式传输数据(TCP 协议)的发送与接收的过滤. 在主功能号为 IRP_MJ_INTERNAL_DEVICE_CONTROL,次功能号为 TDI_SEND_DATAGRAM 和 TDI_RECEIVE_DATAGRAM 的 IRP 对应的派遣函数中实现报式传输数据(UDP 协议)的过滤.

在网络驱动程序中,相关的数据信息的获取主要借助 IRP 的指针,从 PIRP->FileObjec 中可以得到网络连接的 Context 指针、地址、端口等各种信息,从 PIRP->MdlAddress 中可以获取发送或接收数据的 MDL 的指针. 利用这些指针,就可以获取到发送和接收过程的数据,进而按照图书馆网络系统安全监控的策略,对其进行各种操作. 比如检查数据是否符合要求,是否需要对数据进行加密或解密,是否要对数据进行修改,是否要添加校验位,是否对发送或接收的重要数据进行备份,接收或发送的数据是否禁止进一步操作等.

## 4 结论

随着网络技术的普遍应用,高等学校图书馆的服务范围逐步从普通的纸质平台向网络平台扩展. 但是在这一过程中,网络信息安全是高校图书馆必须面对的一个重要课题. 笔者提出了在高校图书馆的网络控

制中，借助网络过滤驱动技术，实现了对各种来自应用层的网络通信行为进行监控，并讨论了其工作原理和具体实现. 此技术可以广泛的用于图书馆网络系统的安全监控、数据监控和行为控制等领域，这在图书馆网络系统安全监控应用领域中具有广泛的借鉴和参考价值.

**参考文献：**


[1] 马　敏，刘兰芳，宁娇丽. 高校数字图书馆网络安全风险分析与策略 [J]. 中国安全科学学报，2010(4)：130－135.

[2] 金文新. 高校图书馆计算机网络系统安全策略的设计与实现 [J]. 图书馆论坛，2009(3)：80－83.

[3] WALTER ONEY. Programming the Microsoft Windows Driver Mode [EB/OL]. [2011－05－26]. http://download.csdn.net/source/353955.

[4] 张　帆，史彩成. Windows 驱动开发技术详解 [M]. 北京：电子工业出版社，2008.

[5] 朱涛江，卢　昱，王　宇. 基于 TDI 的网络安全存储系统研究与实现 [J]. 华中科技大学学报，2003(10)：126－128.

[6] 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.


## Research on Security Monitor of the Library Network System Based on Filter Drive


HOU Chun-ming[1]，WANG Ling[2]

(1. College of Information Science and Information Engineering，Jishou University，Jishou 416000，Hunan China；
2. Library of Jishou University，Jishou 416000，Hunan China)



**Abstract**：The current situation of network security of university libraries is discussed，and the basic principle of network filter driver is introduced. In the Windows operating system，the network filter driver program of WDM is designed，which is attached to the TDI interface to realize the network data filtrating. The realization of this technology has much value to network system security of university library.



**Key words**：filter drive；TDI；network security


（责任编辑　陈炳权）

（上接第 14 页）


[7] YANG F Q，SUN TEL，ZHANG C H. An Efficient Hybrid Data Clustering Method Based on K-Harmonic Means and Particle Swarm Optimization [J]. Expert Systems with Applications，2009，36(6)：9 847.

[8] 于　娟，韩建民，郭腾芳，等. 基于聚类的高效 k－匿名化算法 [J]. 计算机研究及发展，2009(Z2)：46－49.

[9] WU Tie-fen. Application of a New Fuzzy Clustering Algorithm in Intrusion Detection [J]. Modern Electronic Techniuqe，2008(4)：100－102.

[10] LOUKIDES GRIGORIOS，SHAO Jian-hua. An Efficient Clustering Algorithm for k-Anonymisation [J]. Journal of Computer Science and Technology，2008(2)：26－40.

[11] 李柏年. 模糊数学及其应用 [M]. 合肥：合肥工业大学出版社，2007.

[12] 梁保松，曹殿立. 模糊数学及其应用 [M]. 北京：科学出版社，2007.


## Improved Algorithm of Agglomerative Hierarchical Clustering


LIU Wen-jun，YOU Xing-zhong

(Department of Mathematics and Computing Science，Changsha University of Science and Technology，Changsha 410076，China)



**Abstract**：Problems in agglomerative hierarchical clustering method are preseated when Euclid or Minkowski distance is the distance measure，and the causes for those problems are explored. Accordingly，an improved agglomerative hierarchical clustering algorithm according to the idea of fuzzy clustring is put forward. The reasonability and validity of this improved algorithm are proved through an example.



**Key words**：data mining；clustering；distance；algorithm


（责任编辑　向阳洁）