# 基于 Windowns 环境下的 NPF 数据捕获技术的研究*)

张 军[1] 王建华[1] 刘禹麟[2] 张冰雪[1]

(哈尔滨师范大学计算机科学系 哈尔滨150025)[1] (中国人民解放军73011部队 浙江 湖洲313006)

**摘 要** 网络数据包截获机制是网络入侵检测系统的基础部件,本文着重研究基于 Windowns 平台下的 NPF 数据捕获技术。

**关键词** NPF,Winpcap,入侵检测

## The Research of NPF Data Acquisition Technology on Windows Platform

ZHANG Jun[1] WANG Jian-Hua[1] LIU Yu-Lin[2] ZHANG Bing-Xue[1]

(Department of Computer Science,Haerbin Normal University,Haerbin 150025)[1] (The Chinese People's Liberation Army 73011 Army 313006)[2]

**Abstract** Network data packet capturing mechanism is a fundamental component of Network Intrusion Detection System. This paper focuses on the research of NPF Data Acquisition techonlogy on Windows Platform.

**Keywords** NPF,Winpcap,Intrusion detection

## 1 引言

在实际应用中,有时网络的流量会大得惊人,过滤模块的效率就成为网络监听的关键,因为对于网络上的每一数据包都会使用该模块处理,判断是否符合过滤条件。低效率的过滤程序来不及分析处理,会导致数据包丢失。

我们之所以研究 NPF 的捕获过滤模型,就是从提高系统性能的角度出发的,通过深入地理解和运用模型的工作机制进行数据包的采集和过滤,从而开发出高效可靠的网络监控系统。

## 2 Windows 环境下的捕获过滤模型

BPF 已被证明为一个强大稳定的结构,NPF 作为 BPF 在 Windows 环境下的演化版继承了 BPF 的以下重要模块:过滤器,两级缓冲(核心和用户)以及用户级的一些函数库。NPF 的捕获过滤机制如图1所示。

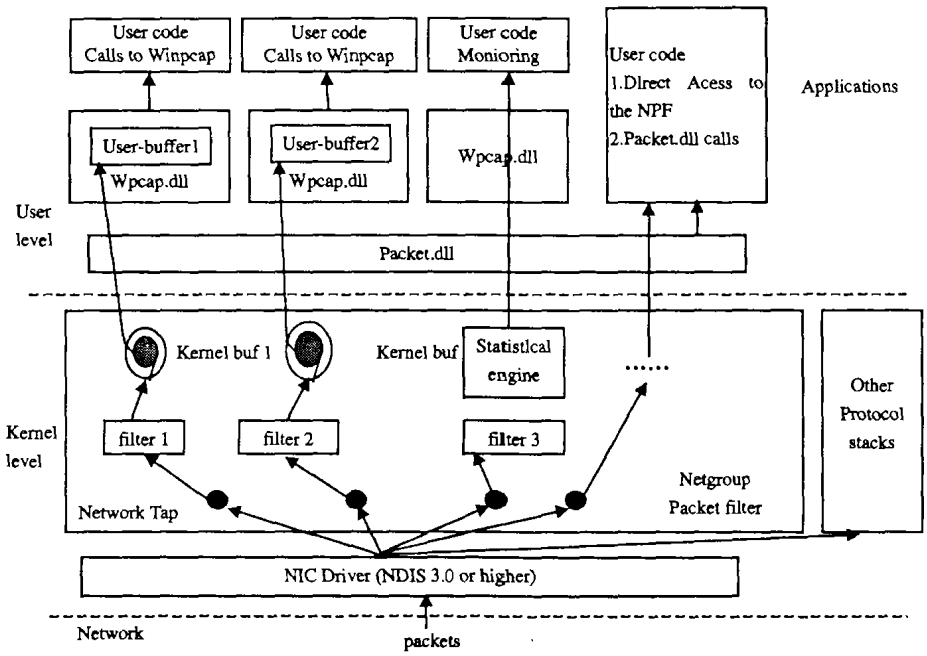


图1 NPF 的捕获过滤机制

NPF 与 BPF 之间的一个重要的结构上的差异是 NPF 选择了循环的缓冲区作为核心缓冲区。循环缓冲区已经被优化成每次可以拷贝几块数据包。这种缓冲实现机制允许所有的核心内存都被用于存储网络中的包,而像 BPF 那样的靠两个缓冲区交换的工作机制只允许一半的内存用来存储网络包。

NPF 中实现了一个核心级的可编程的统计引擎,该引擎

*)获黑龙江省教育厅科研项目资助(10541093),2004年度哈尔滨师范大学校科研基金项目资助.张 军 副教授,主要研究方向:网络安全,计算机辅助教学等.

不再是一个简单的包过滤器，而具有强大的分类功能。应用程序可以命令这个模块监听网络活动的任意方面（例如网络流量，每秒请求 Web 数等），并且等待预先定义的间隔后从核心接收统计结果。

## 3 NPF 模型监听流程

### 3.1 WinPcap 体系结构

NPF 主要用于 Windows 系统平台，但 Windows 系统没有像 Unix 系统一样将捕获过滤机制内置于操作系统，所以需要安装 NPF 系统包。WinPcap 就是这样的驱动安装包，该安装包在系统中安装了三个文件：高级系统无关库（Wpcap.dll）、低级动态链接库（Packet.dll）和内核级的数据包监听设备驱动程序（Npf.sys/Npf.vxd）。这三个文件的层次依赖关系如图2所示。

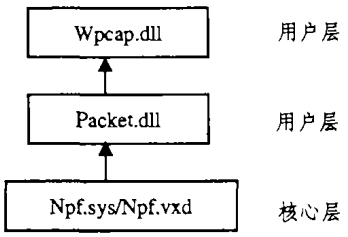


图2 Winpcap 层次依赖关系

①Npf.sys/Npf.vxd：是一个虚拟设备驱动程序。其功能是过滤数据包，并把这些数据包原封不动地传给用户态模块，这个过程中包括了一些操作系统特有的代码。

②Packet.dll：该动态链接库为 Win32平台提供了一个公共接口。

③Wpcap.dll：该动态链接库提供了一个不依赖于操作系统类型的高层接口库，提供了更加高层、抽象的函数。

### 3.2 Packet.dll 的监听流程

使用 Packet.dll 接口的监听程序流程大致如图3所示。

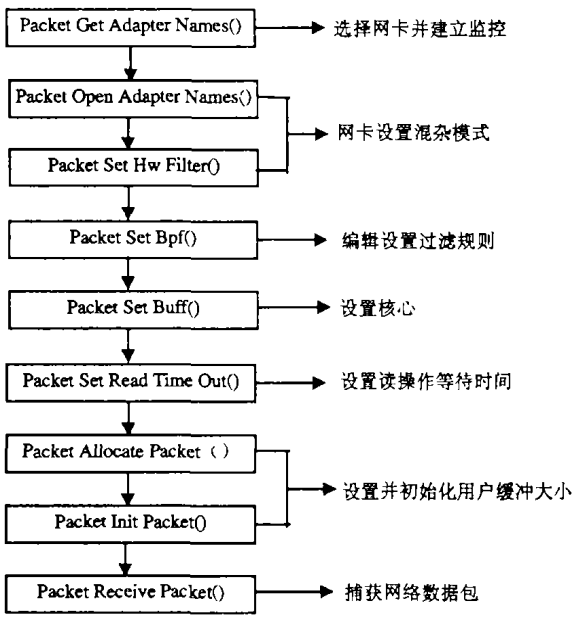


图3 Packet.dll 接口的监听程序流程

### 3.3 Wpcap.dll 的监听流程

使用 Wpcap.dll 接口的监听程序流程大致如图4所示，其中用户对数据包的处理程序可以通过 callback 回调函数实现：

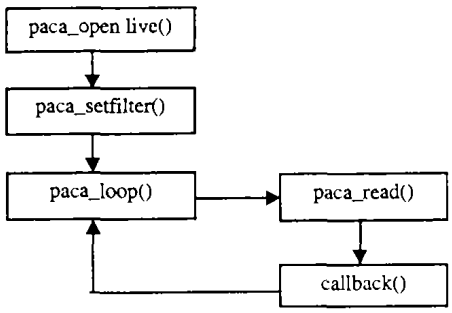


图4 使用 Wpcap 接口的监听程序流程

下面程序给出利用 Wpcap.dll 接口对网络数据包进行监听的简单示例：

```
#include <pcap.h>
#include <stdio.h>
  int main()
  {
   pcap_t *handle;/*监听会话句柄*/
   char *dev; /*监听网络接口*/
   char errbuf [PCAP_ERRBUF SIZE]; /*错误代码*/
   struct bpf_program filter;/*编译后过滤器表达式*/
   char filter_app[ ]= "port 23";/*指定过滤条件*/
   bpf_u_int32 mask; /*网络接口掩码*/
   bpf_u_int32 net;/*网络接口地址*/
   dev=pcap_lookupdev(errbut); /*自动选择网络接口*/
   pcap_lookupnet(dev,&net,&mask,errbuf);/*获取指定网络设
     备的网络地址和掩码*/
   handle=pcap_open_live(dev,BUFSIZ,1,0,errbuf); /*建立监
     听会话*/
   pcap_compile(handle,&filter,filter_app,0,net); /*编辑过滤器
     */
   pcap_setfilter(handle,&filter); /*设置过滤器*/
   pcap_loop(handle,-1,dispatcher_handler,(const u_char *)han-
     dle);/*循环捕获并处理合乎过滤要求的包，直到错误发生*/
   pcap_close(handle); /*关闭监听会话*/
   return(0);
}
    void dispatcher_handler(u_char *uhandle,const struct pcap_
pkthdr *pkthdr,const u_char *pkt) /*对捕获的每一个数据包调
    用该回调函数对数据包进行处理*/
  {
  …… /*协议分析的代码*/
}
```

**结论** NPF 机制为 Windowns 系统平台提供了一套标准的数据包截获接口，并与 libpcap 库兼容，可使得原来许多的 UNIX，Linux 平台下的网络分析工具能快速移植过来。同时 NPF 还考虑了各种性能和效率的优化，如 NPF 内核层次上的过滤器支持内核态的统计模式，提供了直接发送数据包的能力。

## 参 考 文 献


1 唐正军. 入侵检测技术导论. 机械工业出版社，2004

2 谭思亮. 监听与隐藏：网络侦听与数据保护技术[M]. 北京：人民邮电出版社，2002

3 高峻，吕述望. 入侵检测系统（IDS）及其通信协议. 计算机工程，2002(6)

4 Black U. TCP/IP and Related Protocols. New York, NY: McGraw-Hill, Inc., 1992

5 Feit S. TCP/IP: Architecture, Protocols, and Implementation. New York, NY: McGraw-Hill, Inc., 1993

6 Autonomous Agents for Intrusion Detection. http://www.cerias.purdue.edu/about/projects/aafid

7 Deri L, Suin S, Maselli G. Design and implementation of an anomaly detection system:an empirical approach[ J/OL]. http://luca. ntop. org/ADS. pdf. 2001(8)

8 唐正军. 网络入侵检测系统的设计与实现[M]. 北京：电子工业出版社，2002