基于 winpcap 的网络抓包系统

刘飞，杨飞
（四川大学 计算机（软件）学院，成都 610207 ）

摘要：为了监控计算机当前网络信息，我们主要通过使用 winpcap 抓取当前计算机网络中使用的数据包，然后通过对抓取数据包中数据进行分析过滤，得到所抓数据包的协议、数据长度，以及 http 中的数据报内容等信息。此外，我们的项目还注重研究，主要体现在应用层协议的识别方面，同时采用了基于正则表达式技术得到某种应用层协议的特征表达式，然后通过利用正则表达式匹配引擎进行识别。

关键词：数据包；winpcap；网络协议
中图分类号：TP311 **文献标识码**：A **文章编号**：1007-9599 (2012) 08-0132-02

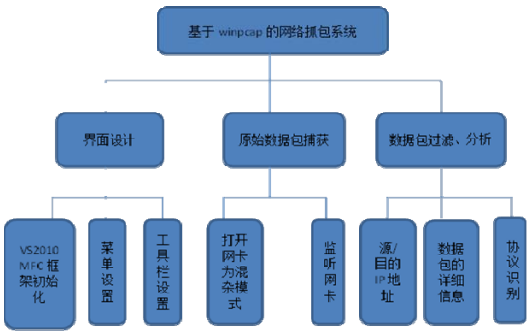
一、引言

如今，随着网络流量的增大，网络安全问题已然越来越不容忽视。为了保障网络不受到恶意攻击，就必须对计算机接收到或发送的网络数据包进行研究，因此网络原始数据包的捕获和对数据包的解析显的尤其重要。本文主要讲解了如何利用 winpcap 实现一个网络抓包系统。

二、具体实现

（一）系统设计

基于 winpcap 的网络抓包系统的功能模块如图 2-1 所示：



1.界面设计模块。在这部分主要做的工作是 VS、MFC 框架的初始化，界面中的主要菜单和工具栏的设置，本系统主要采用 ribbon 界面。

2.原始数据包捕获模块。该模块的包括获取设备列表，跳转到选中的适配器，打开网卡为混杂模式，释放设备列表，监听网卡开始捕获。

3.数据包分析过滤、分析模块。该模块是系统的核心部分，是对协议的识别和对数据包中所包含的信息的解析，如源、目的 IP 地址、源/目的端口号、信息长度等。

（二）原始数据包捕获

原始数据包的捕获有很多种方法，我们常用的有两种，一种是使用原始套接字，另一种是使用winpcap(windows packet capture)开发包。Winpcap是win32 平台下一个免费，公共的网络访问系统，它由数据包捕获驱动、底层动态链接库(Packet.dll)和高层静态链接库(wpcap.lib)三部分组成 [0]。Winpacap提供了以下功能：

捕获原始数据包，无论它是发往某台机器的，还是在其他设备（共享媒介）上进行交换的

在数据包发送给某应用程序前，根据用户指定的规则过滤数据包

将原始数据包通过网络发送出去

收集并统计网络流量信息

我们选择 winpcap 是因为它不仅有着高性能而且容易理解，具有可移植性等优点。

使用 winpcap 捕获数据包的流程：

➢ 获取设备列表

```
pcap_if_t* alldevs; //指向网卡设备的指针
pcap_if_t* d;
char errbuf[PCAP_ERRBUF_SIZE];
//获取网络设备指针
pcap_findalldevs(&alldevs,errbuf);
for(d=alldevs;d;d=d->next)  //枚举网卡
d->name; //网卡的名字
```

➢ 打开网卡并设为混杂模式

网卡具有如下的几种工作模式：

1.广播模式（Broad Cast Model）:它的物理地址（MAC）地址是 0Xffffff 的帧为广播帧，工作在广播模式的网卡接收广播帧。

2.多播传送（MultiCast Model）：多播传送地址作为目的物理地址的帧可以被组内的其它主机同时接收，而组外主机却接收不到。但是，如果将网卡设置为多播传送模式，它可以接收所有的多播传送帧，而不论它是不是组内成员。

3 直接模式（Direct Model）：工作在直接模式下的网卡只接收目地址是自己 Mac 地址的帧。

4.混杂模式（Promiscuous Model）：工作在混杂模式下的网卡接收所有的流过网卡的帧，信包捕获程序就是在这种模式下运行的。

网卡的缺省工作模式包含广播模式和直接模式，即在通常情况下，应用程序无法收取与自己无关的数据包。所以我们要想实现截获流经网络设备的所有数据包，就要采取一点特别的手段了：即将网卡设置为混杂模式。这样一来，该主机的网卡就可以捕获到所有流经其网卡的数据包和帧。

```
pcap_t* adhandle;
if((adhandle=pcap_open(d->name, //设备名
65535,  /*65535 保证能
捕获到不同数据链路层上的每个数据包的全部内容*/
PCAP_OPENFLAG_PROMISCUOUS,  //混杂模式
1000,  //读取超时时间
NULL,  //远程机器验证
errbuf))==NULL)
{
fprintf(stderr,"\nUnable to open the adapter. %s is not supported by WinPcap\n", d->name);
        /* 释放设备列表 */
pcap_freealldevs(alldevs);
return -1;
}
```

➢ 捕获数据包并保存

```
pcap_dumper_t *dumpfile;
/* 打开堆文件 */
dumpfile=pcap_dump_open(adhandle, "pkt.dat");
/* 开始捕获 */
pcap_loop(adhandle, 0, packet_handler,
(unsigned char *)dumpfile);
   /* 回调函数，用来处理数据包 */
void packet_handler(u_char *dumpfile,
const struct pcap_pkthdr *header,
const u_char *pkt_data)
{
       /* 保存数据包到堆文件 */
       pcap_dump(dumpfile, header, pkt_data);
}
```

（三）数据包分析与过滤

数据包的分析主要采取如图 2-2 所示的步骤，

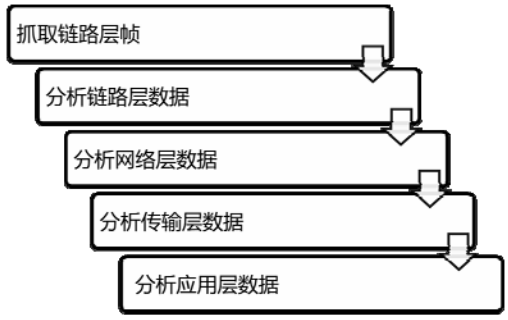


图 2-2 数据包分析步骤

首先，我们根据数据包的头部自定义相应的结构体，然后进行解析。对应用层协议的识别是我们重点关注的地方。对于如今比较流行的网络抓包软件 wireshark 来说，它是基于端口号来识别的，例如：默认将来自 80、3128、3132、8080、8088、11371、1900 端口的数据识别为 HTTP 协议。还有一种方法是基于正则表达式识别，通过大量的统计分析，得到某种应用层协议的特征表达式，然后利用正则表达式匹配引擎进行识别。它们两者各有优缺点，基于端口号的识别虽然效率比较高，但是对于一些不常见的协议不容易识别出来。而基于正则表达式的识别对应用层协议的识别范围比较广。

我们的系统结合了上述这两种方法，利用各自的优点。我们自己研究出来一些协议的正则表达式。尤其对 DNS 的识别率达到 100%。

三、结论与分析

随着计算机网络的飞速发展，网络抓包的应用越来越多，如实时监控网络流量，当出现网络异常时及时的分析出问题所在，分析网络协议，避免网络攻击等。本系统通过使用 winpcap 驱动包，实现了数据包的捕获，并对其进行了相应的分析。但是系统还存在缺点，那就是对数据包的分析还不够完善，这是进一步工作的重点。

参考文献：

[1]林辉,朱俊平.基于WinPcap的数据捕获系统[J].科技信息,2011,No.11,I0076-I0076,I0098

[2]赵亚景,李太浩.基于WinpCap的网络流量监测系统的研究与设计[J].农业网络信息,2010,No.12,29-30

[3]徐鹤,王汝传.一种P2P流量监控系统的设计及实现[J].计算机技术与发展,2009,Vol.9,No.10,6-10

[4]刘捷,朱程荣,熊齐邦.分布式网络自动抓包管理系统的设计与实现[J].计算机工程与设计,2009,30(22),5091-5093

[作者简介]刘飞（1991.6-），男，湖北、荆门，学历：学士。研究方向：软件工程和软件测试。

杨飞（1989,3-），男，河南、信阳，学历：学士。研究方向：图形图像处理和人工智能。

（上接第 134 页）

数的鼠标消息进行返回，对 Hook 监视进行使用，将其输入到鼠标消息中。依据 Hook 的技术规范，Hook API 要写在 DLL 中，在主程序中，进行 Hook 函数的调用。

3.通过 Screen2Bitmap 和 Bmp2Stream 两个函数的应用，可实现程序的屏幕抓取。Screen2Bitmap 可对屏幕进行截取，并将图片进行保存，之后在返回到位图的句柄当中；Bmp2Stream 可对位图句柄进行接收，并对这一个位图进行有效的编码，在将其进行拷贝后保存在缓冲区里。在服务器端，程序会通过屏幕的抓取命令对客户端进行图像的截取要求，如尝试失败，就会返回，反之，就会 len 参数中进行图像数据的传递，之后服务器端来完成图像数据的接收。

三、结束语

总而言之，实现局域网计算机活动的监控，是有效地通过 Internet 技术，在 TCP / IP 协议的基础之上，对软件结构进行合理的组织，而用户对电脑运行情况的了解则是通过局域网内的监控系统来实现的。其监控系统的客户端主要通过钩子技术、多线程技术、SOCKET 技术的应用，在 C / S 模式中有效地进行计算机的监控。客户端进行信息的收集，并将信息发送给服务端，在完整的呈现给管理人员，整个过程都在监控系统的进行下有序良好的进行，使管理人员在局域网内能够实现正常的管理和监测，进而促使了计算机管理的准确性和高效性。

参考文献：

[1]刘海林,陈世欣,龚仕华.基于 HOOK 技术的计算机监控系统设计与实现[J].广东技术师范学院学报,2008(12):1-3

[2]杨竹青.基于 HOOK 技术的实验室软件监控系统研究[J].职业技术学院学报,2009(13):1-3

[3]李统林,刘天时,基于钩子技术的操作监控系统设计[J].淮阴工学院学报,2008(17):1-4

[4]韩红章,王波.局域网内计算机活动监控系统的设计与实现[J].电脑知识与技术,2008（4）: