学校编码：10384　　分类号_____密级_____

学号：X200128032　　UDC _____

学　位　论　文

Windows 环境网络封包截获技术研究

Research the technology of network package capturing in Windows environment

朱元忠

指 导 教 师 ： 倪子伟　副教授

申 请 学 位 类 别 ： 硕 士

专 业 名 称 ： 计 算 机 应 用

论 文 提 交 日 期 ： 2005 年 4 月

论 文 答 辩 日 期 ： 2005 年 5 月

学 位 授 予 单 位 ： 厦 门 大 学

学 位 授 予 日 期 ： 2005 年 月 日

答辩委员会主席:

评　　阅　　人:

二〇〇五年四月

摘要

当前，网络应用逐步深入到社会生活的各个角落，随着电子商务、电子政务等应用的深入，网络的安全日益成为人们关注的焦点。必需承认，当前的网络充满着各种安全隐患，木马程序广泛传播、时时进行更新的病毒、频频曝光的后门漏洞及恶意的入侵事件使得网络应用受到了许多的制约。因此与网络安全相关的编程技术受到了极大的关注，而封包截获是编写各种网络安全程序的基础，因此研究封包截获技术具有现实的意义，目前在书籍及网络中讨论的较多的是 UNIX 和 LINUX 环境下的封包截获技术，而对于使用最多的操作系统 WINDOWS 环境中的封包截获的实现研究的并不是很多，所以这里主要对 WINDOWS 环境下的封包截获技术进行讨论。

WINDOWS 环境中的封包截获技术有多种方法，比如传输过滤驱动、NDIS 中间层驱动程序的编写，这些方法由于涉及到了驱动程序的编写，因此具有相当的难度。另外在最新版的 WINSOCK 2 中提供了一种新的编程接口即 SPI，采用该技术可以方便的在应用层中插入自己的一层处理，这样使得网络封包截获地实现变得相对简单了。另外，系统无关捕获函数库的出现，更使得封包的捕获变得容易了，由于系统无关捕获函数库既有在 LINUX 下的版本，也有在 WINDOWS 下的版本，它们具有很强的兼容性，应用这个函数库就可以较为容易的编写跨平台的网络应用程序。

本论文主要介绍了以下内容：

第一章介绍了计算机安全、网络安全的一些基本概念及相关术语以及探讨 WINDOWS 环境中网络封包截获的意义。

第二章介绍了 WINDOWS 网络结构的协议框架。

第三章介绍了 WINDOWS 环境下网络封包截获的原理及实现方法。

第四章给出了一个具体的应用前面介绍的方法实现的数据封包截获程序的简单模型

第五章简单介绍了研究网络封包截获技术给工作学习方面带来的启迪。

本文的贡献主要是以下几个方面：

1. 本文从技术研究联系到我院计算机网络专业的建设，提出了技术研究对专业建设和专业课程开发的重要意义。

2. 详细分析了各种网络封包截获技术的实现方法及技术要点，并讨论了各种技术的优缺点及应用场合，对于编写与网络数据包截获与过滤程序有重要的借鉴意义。

3.建立了一个完整的截获网络包的演示程序。演示了使用网络封包截获技术截获数据的整个过程。

关键词：网络数据封包截获，传输驱动程序，NDIS，SPI， WinPcap

ABSTRACT

Network application goes deeply into every corner of society life step by step currently. With the development of the application of e-business and e-government, the network security becomes the focus that people take care of more and more. We must admit that network is filled with many security troubles. Hobbyhorse program, computer virus, backdoor hole, and the events of inbreak, all of these restrict the applications of network badly. So the programming technology on network security arouses people's attention. The packet capture, as the base of network security programming, has some important meanings to us. In books and network people talk much about the packet capture based on Linux and Unix, but the realization in Windows, a widely used operating system, is very few. This article mainly reearches the packet capture in Windows environment.

The realization of packet capture in windows environment has many ways. Such as TDI, NDIS Intermidate Driver (IMD), because these ways come down to the programming of driver program, they are very difficulty. Otherwise the best version of Winsock 2 offers a new programming interface — SPI, we can use this technology to insert an owner layer of process in the application layer. This will make the network packet capture easily. The appearance of the system independent capture library makes packet capture easier than ever. Because there are both versions of Windows (WinPcap) and Linux (Libcap) and they are compatible to each other, we can use the library easily to program network application program for different OS.

This article mainly discusse the following contents:

In chapter 1, the related concepts are introduced, such as Computer Security, Network Security and packet capture.

In chapter 2, the protocol frames of Windows network structure are described.

In chapter 3, the theory and the realization way about network packet capture in the Windows environment are expounds in some detail.

In chapter 4, a sample about how to capture packet is given and analyzed. The

sample uses the theory and the way that are dicussed in the preceding chapters.

In chapter 5, some important edification about the research of network packet capture is summaried.

This thesis has the following contributions:

- The article, relating from the technology research to the network specialty building of our institute, brings forward that the technology research have very important effects for the specialty building and the course exploiture of specialty .
- The article analyses the realization ways and the key point on many technologies of network packet capture. It also discusses the advantage, disadvantages and application occasions about every kind of technology. They can be referenced for the programming of the network packet capture and filter.
- The article establishes a demo program to capture network packet. The program gives the entire process to capture data packet by using the technology of packet capture.

Keywords：Network packet capture; Transfer driver; Network Driver Interface Specification ; Service Provide Interface; WinPcap

目录

第一章 概述

1.1 计算机安全研究的内容

1.1.1 计算机安全技术的含义

计算机安全技术主要包含以下几个方面的含义:

1)保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。信息经过加密变换后变成密文，只有那些经过授权的合法用户，掌握解密密钥，才能通过解密算法将密文还原成明文。

2）完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

3）可用性：可被授权实体访问并按需求使用的特性。安全系统能够对用户授权提供其某些服务，即经过授权的用户可以得到系统资源，并且能享受系统所提供的服务。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。

4)可控性：对信息的传播及内容具有控制能力。

5)可靠性：可靠性是指对信息完整性的依赖程度，也是对信息安全系统完整性的依赖程度。

1.1.2 计算机安全的主要研究内容

1. 物理安全

计算机系统物理安全主要是指为保证计算机设备和通信线路及设施（建筑物等）的安全。一是预防地震，雷电等自然灾害，满足设备正常运行环境的要求而采用的技术和方法；二是采取必要的措施防止计算机设备被盗，设定安全管理规定；三是为防止电磁辐射泄漏而采取的低辐射产品、屏蔽或反辐射技术和各种设备的备份等。

2. 密码学

密码学是一门研究密码系统或通信安全的科学。它主要包括两个分支，密码

编码学和密码分析学。密码编码学的主要目的是寻求信息保密性和可认证性的方法，密码分析学的主要目的是研究加密消息的破译和信息的伪造。这两个方向相互联系，相互促进。

3. 操作系统安全

操作系统是计算机重要的系统软件，它控制和管理计算机所有的软、硬件资源。由于操作系统的重要地位，使攻击者常常以操作系统为主要攻击目标，因此研究保护操作系统的方法、设计安全的操作系统，对整个计算机系统的安全至关重要。操作系统采用的安全控制方法主要是隔离控制和访问控制。

4. 数据库安全

数据库安全指的是为了保护计算机系统中数据库（或数据文件）免遭破坏、修改、显露和窃取等威胁和攻击而采用的技术方法，包括各种用户识别技术、口令验证技术、存取控制技术和数据加密技术，以及备份、异地存放、妥善保管等技术和方法。

5. 网络安全

计算机网络就是将分散在不同地理位置的计算机系统，通过某种介质连接起来，实现信息的资源的共享，Internet 的迅速发展给网络系统的安全保护提出了更高的要求。网络安全是指网络系统的部件、程序、数据的安全性，它通过网络信息的存储、传输和使用过程体现。所谓的网络安全性就是保护网络程序、数据或者设备，使其免受非授权使用或访问，它的保护内容包括：保护信息和资源，保护客户和用户，保证私有性。网络安全是计算机安全的一个重要组成部分。

6. 病毒防治

计算机病毒是一种危害极大的程序，它直接威胁着计算机系统的安全。它在一定的条件下激发，感染磁盘引导区，或数据文件与程序，占用系统资源，降低系统效率，重者造成整个系统的瘫痪。因此研究计算机病毒的种类，原理，检测与清除技术是计算机安全的重要组成部分。

1.1.3 计算机安全标准及机构

1、美国国家安全局 NSA

美国国家安全局简称 NSA（National Security Agency），是美国政府的官方安全机构，该机构建立于 1952 年，隶属于美国国防部。它的主要任务是监听和破译所有对本国信息安全有价值的外国通信。

NSA 还一直从事密码学的研究，一方面研究密码算法，加强本国通信的安全；另一方面研究密码分析技术，监听他国的通信。NSA 被世界公认为是拥有最多的数学家的机构，也是先进计算机设备的最大买主，因此，NSA 在密码学研究领域总是处于领先地位，许多实际应用的密码系统都分别被其击破。

2、美国国家计算机安全协会 NCSA

美国国家计算机安全协会简称 NCSA（National Computer Security Association），它是 NSA 的一个分支机构，担负着国家重要的计算机程序设计工作。该协会负责对商业性的安全产品进行评估，包括硬件产品和软件产品的评估，主持重点项目的研究工作，开展技术指导咨询，提供建议方案，并且组织培训服务。

NSCA 成功地制定出国防部计算机系统的评估准则 DDTCSEC（Department of Defense Trusted Computer System Evaluation Criteria），准则中将安全的可靠性分成 A，B，C，D 四类 8 个等级，具体如下：

D：最低安全要求，属非安全保护类，它不能用于多用户环境下的敏感信息的处理。只有一个级别。

C：自主型保护类，它分为两级

C1：具有一定的自主型存取控制机制，通过用户与数据隔离措施满足安全要求。

C2：可控制的安全保护机制，通过注册、审查、资源隔离达到安全要求。

B：强制型安全保护类，它分为三级

B1：标记安全保护，具有 C2 级的全部功能，并增加了标记强制型访问控制等功能。

B2：具有形式化安全模型，系统设计结构化，并要求计算机系统加人一种允许用户去评价系统满足哪一级的方法。

B3：安全区域级，具有严格的系统结构化设计，并具备全面的存取控制的访问监控机制，以及审计报告机制。

A:验证型安全保护类，分两级

A1；验证设计，要求用形式化设计说明和验证方法对系统进行分析。

超 A1：验证客观级，比 A1 级具有更高的安全可信度要求，其技术有

待于今后进一步研究探讨。

1.2 网络安全的基本概念

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全是指网络系统的部件、程序、数据的安全性，它通过网络信息的存储、传输和使用过程体现。网络安全包括物理安全和逻辑安全。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。确保网络系统的信息安全是网络安全的目标，信息安全包括两个方面：信息的存储安全和信息的传输安全。信息的存储安全是指信息在静态存放状态下的安全，如是否会被非授权调用等。信息的传输安全是指信息在动态传输过程中安全。为了确保网络信息的传输安全，有以下几个问题：

（1）对网络上信息的监听

（2）对用户身份的仿冒

（3）对网络上信息的篡改

（4）对发出的信息予以否认

（5）对信息进行重发

网络的安全威胁主要有三个来源：

(1) 人为的无意失误

(2) 人为的恶意攻击

(3) 网络软件的漏洞和“后门”

网络安全的威胁主要包括如下几种类型：

(1)物理威胁：偷窃、废物搜寻、间谍行为、身份识别错误

(2)线缆连接：窃听、拨号进入、冒名顶替。

(3)身份鉴别：口令圈套、口令破解、算法考虑不周、编辑口令

(4)编程：

A 病毒：Internet 蠕虫

B 代码炸弹：一旦到了设定的时间，它就被触发并产生破坏

C 特洛伊木马：特洛伊木马是包括病毒、代码炸弹、蠕虫和诸如此类的恶意代码的通称。

D 更新或下载：有些网络允许通过 MODEM 进行操作系统更新，于是非法闯入者通过它对系统进行非法更新。

E 系统漏洞：亦称为陷阱，通常由系统开发者有意设置的，能在用户失去了对系统的所有访问权后仍进入系统。

1.3 研究 Windows 环境下的网络数据封包截获机制的意义

Windows 操作系统一直以绝对的优势占据着个人计算机市场，而且这种优势还在继续保持，与 Windows 相关的软件产业，自然也就备受关注。另一个方面，由于网络的迅速崛起，出现了传统的软件产业跟不上网络发展的状况，所以传统的软件产业应该尽快向网络靠拢。目前，网络游戏的空前火爆制造了一个巨大的利润场，吸引着国内许多的软件企业涉足其中，对于网络编程是一个巨大的促进，这种形势使得网络编程成为较热门的编程技术，熟练掌握 Windows 网络编程技术的人已经成为炙手可热的人才。

而在网络应用遍及的今天，信息泄漏、病毒横行以及防不胜防的木马程序，这些频频发生的网络安全问题使人们对网络的应用前景产生了不安。网络有没有安全，如何保障网络的安全，是许多网络应用这继续找到的答案。为了保障网络的安全，许许多多的网络安全产品应运而生，如防火墙软件、入侵检测系统、网络嗅探器。这些软件的编制都是建立在一种基本的编程技术之上的，那就是网络数据封包截获与过滤技术。现在的许多探讨封包截获技术的书籍及论文通常都讨论的是 Unix 下的实现方法，探讨在 Windows 下实现的书籍较少，在 Windows 环境下网络数据封包的截获与 Unix 系统下的编程机制有些不同，在 Unix 系统中，操作系统提供了包截获的编程接口，而在 Windows 系统中则没有这样的接口，我们需要使用编写设备驱动程序的方法或者是用 WinSock 来实现。研究 Windows 下的网络数据封包截获技术，可以是我们更加清楚的了解到网络数据封包在网络上的传输过程，了解造成网络不安全的许多因素，可以对网络安全工具的工作原理有更加深入的理解，从而可以更加安全的使用网络。不仅如此，我们还可以针对一些具体的应用环境编写一些网络安全工具来帮助我们维护网络的安全。

1.4 本文的主要贡献

本文的贡献主要是以下几个方面：

1. 本文从我院设立计算机网络专业的实际情况出发，结合我院计算机网络专业课程建设与课程开发的需要，探讨在高职计算机网络专业中加入网络安全编程技术的可行性和必要性。

2. 详细分析了各种网络封包截获技术的实现方法及技术要点，并讨论了各种技术的优缺点及应用场合，对于编写与网络数据包截获与过滤程序有一定的借鉴意义。

3. 建立了一个完整的截获网络包的演示程序。演示了使用网络封包截获技术截获数据并对数据封包进行了简单的解码。

第二章 Windows 网络协议框架

2.1 Windows 操作系统的总体框架

Windows 操作系统的总体框架分为两个层次，上面的为应用层，下面的为核心层。如下图所示。

图 2.1Windows 操作系统的架构

应用层是可以直接接触到的，应用程序（.exe）工作在这一层；动态链接库（.dll）也属于应用层的范畴，动态链接库被应用程序调用时就成为应用程序的一部分，所以它们并没有本质的区别。DLL 和 EXE 是两种工作方式不同的应用程序。EXE 是一个独立且可以直接执行的模块，受 Windows 进程保护机制的保护，其它应用程序无权直接使用这个程序的模块和数据。DLL 是一个共享的函数库，它提供标准的接口供其它应用程序调用，本身却不能单独运行。

各种用户界面都是应用程序运行的结果，它们工作在应用层。在应用层下面还有一层叫核心层（kernel）。Windows95/98 下核心层的程序扩展名为.vxd；WindowsNT/2000 下的核心层程序的扩展名为.sys，这些程序叫做驱动程序。驱动程序为上层应用程序提供底层的支持。

这种分层结构可以实现代码共享。以协议驱动程序为例，一个系统里可能有许多程序使用相同的网络协议，把协议驱动程序单独调用出来就可以实现代码的共享。就像 DLL 可以被所有的 EXE 调用一样，所有的应用程序都可以调用同一个协议驱动程序。这样，操作系统就可以使协议对应用程序透明，应用程序不必关心协议的实现方法，只要按提供的接口函数作相应的操作即可。

代码的分层结果出了可以方便代码共享，还可以实现安全保护。因为像协议驱动程序之类的程序对程序的执行效率和代码的严谨性、强壮性要求非常高，一旦程序出现问题，就可能是系统瘫痪，因此将操作系统分为两层，可以分别赋予它们不同的操作权限，应用层程序位于上层，一个应用层程序质量的好坏不会影

响整个系统的运作，所以对应用层程序的要求较低，授予它的权限也较低，在 Windows 保护机制的作用下，应用程序受到许多限制。例如应用程序无权直接操作 CPU，不能直接操作其他应用程序的缓冲区等。核心层的程序就不一样了，它具有与操作系统同等级别的权限，驱动程序几乎可以对所有的资源进行直接的读写操作，包括软硬件。

2.2 开放系统互连参考模型（OSI）

OSI 模型将网络通信结构分为 7 层，从下到上依次为物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）和应用层（Application Layer）。其通信模型如下图所示。

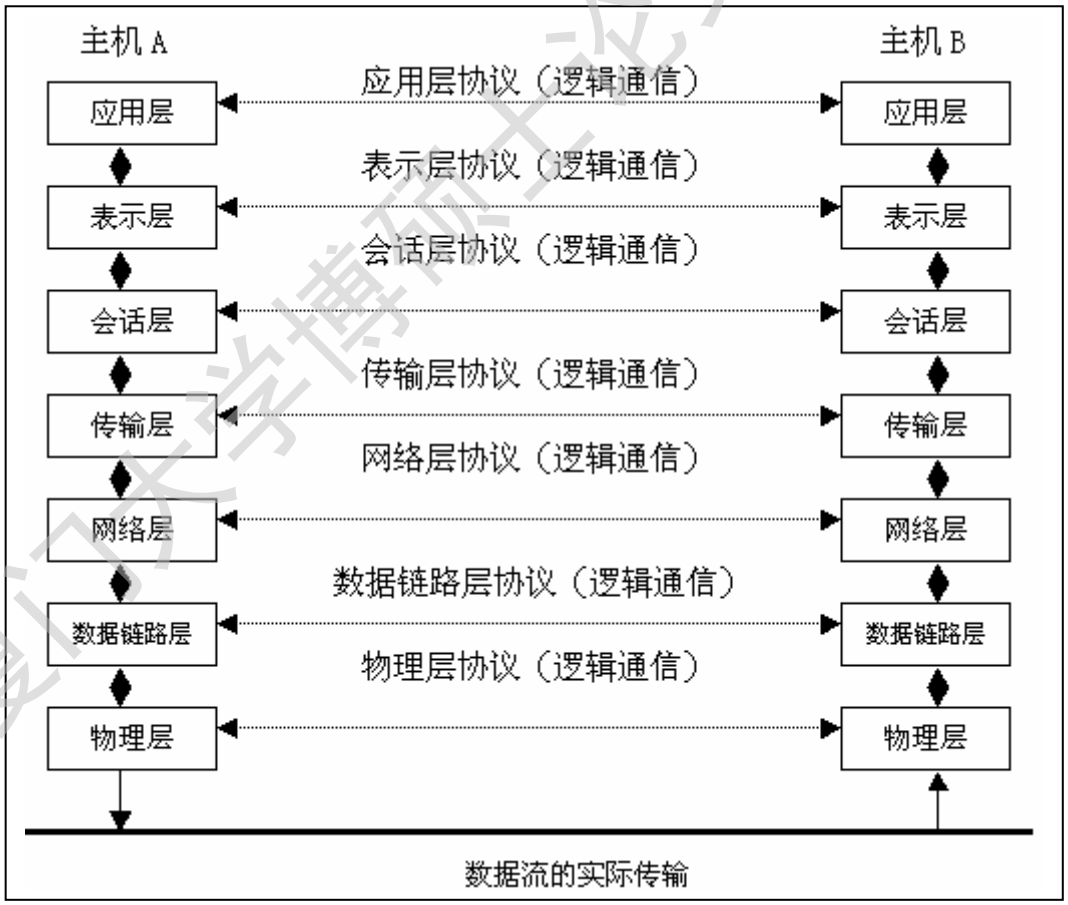

图 2.2 OSI 七层通信模型

OSI 模型中每一层只与其上下两层直接通信。高层协议偏重于处理用户服务和各种应用请求，低层协议偏重于处理实际的信息传输。分层的目的在于把各种特定的功能分离开来，并使其实现对其他层次来说是透明的。这种分层结构使各