计算机专业人员书库

朱雁辉 编著
朱雁冰 审校

Windows 防火墙与网络封包截获技术

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

计算机专业人员书库

Windows 防火墙与网络封包截获技术

朱雁辉　编著
朱雁冰　审校

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书首先论述了各种常用的网络封包截获方法，包括传输层过滤驱动程序、NDIS 中间驱动程序和 Winsock 2 SPI。然后以 Xfilter 个人防火墙为实例，从功能分析、模块设计、文件结构定义、界面设计到编码、制作帮助文件及制作安装盘，完整地介绍了软件开发的全过程。因此，从本书中不仅可以学到较为全面的封包截获技术，而且可以借鉴工程化的方法制作自己的软件。

图书在版编目(CIP)数据

Windows 防火墙与网络封包截获技术/朱雁辉编著 .—北京：电子工业出版社，2002.7
(计算机专业人员书库)
ISBN 7-5053-7717-5

Ⅰ.W… Ⅱ.朱… Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2002)第 040949 号

责任编辑：黄志瑜
特约编辑：李建森
印　　刷：北京东光印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787 x 1 092　1/16　印张：38.5　字数：985.6 千字　附光盘 1 张
版　　次：2002 年 7 月第 1 版　2002 年 7 月第 1 次印刷
印　　数：6 000 册　定价：62.00 元(含光盘)

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。
联系电话：(010)68279077

前　言

随着网络的普及，安全问题正威胁着每一个网络用户。由于黑客攻击和信息泄漏等安全问题并不像病毒那样直截了当地对系统进行破坏，而是故意隐藏自己的行动，所以往往不能引起人们的重视。但是，一旦网络安全问题发生，通常会带来严重的后果。因此，必须加强安全意识，并及早防范。目前最常用的网络安全防范工具是防火墙，相信不用多久，防火墙软件就会像防病毒软件那样安装在每一个人的计算机上。这将产生一个巨大的网络安全市场。作为软件开发者的程序员更要抓住这个机遇，掌握这门专业技术，为自己创造更多的机会。

由于网络安全技术涉及到太多的机密问题，所以这项技术总是以原理的形式出现，具体实现方法很少有人提及。因此，网络安全技术的发展受到了很大阻碍，能够掌握这门技术的专业极人才也非常匮乏。本书首次公开了完整的防火墙源程序和文档，并对关键技术和程序进行了详细的说明。另外，本书的网站 http://www.xfilt.com 作为在线平台会及时地对技术进行跟进和更新，因此本书是学习防火墙和网络编程的理想选择。

主要内容

本书首先论述了常用的各种网络封包截获方法，包括传输层过滤驱动程序、NDIS 中间驱动程序、Winsock 2 SPI。然后以 Xfilter 个人防火墙为实例，从功能分析、模块设计、文件结构定义、界面设计到编码、制作帮助文件及制作安装盘，完整地介绍了软件开发的全过程。因此，从本书中不仅可以学到较为全面的封包截获技术，而且可以借鉴工程化的方法制作自己的软件。

本书的特色

本书从需求分析到打包发布，详尽地介绍了一个软件产品的生产全过程。这些一向被认为是商业机密的资料被首次公开。

本书所使用的实例，是一个精心设计的、完整的个人防火墙软件产品 Xfilter，此外，还有许多精巧实用的实例。Xfilter 是一个具有典型功能的防火墙产品，它最具意义的是公开了完整的源代码。网络安全产品一向以技术含量高、保密性强而著称；公开防火墙的源代码，无疑会给黑客提供更好的机会去创造攻击手段。但是事物总有两面性，事实上，它有更好的一面。它可以帮助广大程序员掌握这门核心技术，以编写更安全的防火墙软件。

本书对示例的讲解有一个显著的特点就是“完整”。为适应基础不同的读者的需要，本书在对示例论述的时候，尽量做到使过程描述完整。

本书的读者

本书适于以下类型的读者阅读。

（1）需要用到网络封包截获技术的读者，这本书能给予很大的帮助。

（2）做网络安全软件开发的读者。有关这方面内容的实例性图书，市面上不多见，这本书是他们所渴望得到的。

（3）刚学了一点 VC 基础，正愁着没有项目试验的读者。这本书不仅可以让你由浅入深地掌握防火墙的开发技术，而且可以成为熟练的 VC 程序员。

（4）需要提高系统分析能力的读者。理解并消化好书里的例子，将增进系统分析经验，提高系统分析的能力。

（5）做软件驱动程序开发的读者。掌握了书中的最小化示例，做驱动程序就像编写“Hello World”一样简单。

（6）计算机专业的同学们，如果你正找不到系统分析的参考资料来做毕业论文，这里面有你想要的资料。

如何阅读本书

本书分为 3 大部分：

第一部分，网络封包截获技术。除了介绍常用的网络封包截获技术外，还加入了 Windows 的网络架构和构建编程环境的相关内容。

第二部分，Xfitler 个人防火墙实例剖析。这一部分包括 Xfilter 个人防火墙的系统设计、代码分析、帮助文件制作、安装盘制作和测试文档等内容。

第三部分，附录。这一部分给出了 Winsock 2 传输服务提供者的 31 个函数的解释以及 Xfilter 使用的宏代码、全局变量和结构类型的说明。

如果想系统地了解各种封包截获方法和实际应用，可以从头到尾地阅读本书，由浅入深地掌握核心技术和实战经验。另外，本书的一些章节有很高的独立性，所以也可以按照需求跳跃式地阅读感兴趣的章节。

（1）如果对 Windows 的核心架构不太了解，建议阅读第 1 章。

（2）如果只对驱动程序截获网络封包感兴趣，可以直接阅读第 3 章和第 4 章。如果在阅读过程中还想创建自己的编程环境来做实验，可以回过头阅读第 2 章。

（3）如果对 Xfilter 的核心技术 Winsock 2 SPI 感兴趣，建议从第 5 章开始顺序阅读。第 5 章是对 Winsock 2 SPI 的基础论述，并且有较为简单的示例，可以作为入门章节。第 6 章是一个完整的 SPI 示例，介绍了如何用 Winsock 2 SPI 技术截获网络封包。第 8 章、第 9 章和第 10 章讲述了 Xfilter 如何利用 Winsock 2 SPI 来完成对网络封包的截获、分析和控管。

（4）如果想了解 Xfilter 的系统设计，则可以直接阅读第 7 章。

（5）如果想整体地把握 Xfilter 技术，最好的办法是完整地阅读 Xfilter 的源代码。在阅读的过程中可充分利用本书的系统分析文档和函数说明，以便用最短的时间掌握最多的知识。

（6）如果只对帮助文件制作感兴趣，则可以直接阅读第 16 章。

（7）如果只对安装盘制作感兴趣，则可以直接阅读第 17 章。

（8）如果已经掌握了 Winsock 2 SPI 技术，只是在实际编程过程中需要实时查阅函数资料，则可以查阅附录 A。

致谢

感谢我的父母，他们不辞劳苦地工作，为我创造了一个温暖而又稳定的环境，让我可以无忧无虑地写作。感谢我的弟弟朱雁冰，他除了帮我搜集资料和校稿外，还为 Xfilter 写了一部分代码。没有他们的帮助就没有这本书的出版，在此向他们表示深深的谢意！另外更要感谢我的好友余超，他为本书提出的真知灼见非常难能可贵。

如果有什么意见或建议，请发送电子邮件到 xstudio@371.net 或 xstudio@xfilt.com。

配套光盘包括的内容

Winsock 2 SPI 相关示例：

（1）MinWinsockSpi

最小化的基础服务提供者及安装例程。

（2）MinLSP

最小化的分层服务提供者及安装例程。

（3）PacketCapture

截获网络封包的基础服务提供者及安装例程。

（4）GuiDesign（VB）

Xfilter 个人防火墙的界面设计。

（5）Xfilter

提供 Xfilter 个人防火墙 1.0.2 版的完整代码。另外，还包含帮助文件制作的源文件、安装程序制作的源文件及完整的安装程序。

DDK 相关的示例：

（1）MinDriver

最小化的驱动程序。

（2）MinDriverInVc

在 VC 中编译最小化的驱动程序。

（3）FilterTdiDriver

截获网络封包的传输层过滤驱动程序。

（4）xpassthru

截获网络封包的 NDIS 中间驱动程序。

相关工具（tools）：

DumpSpi.exe

枚举出系统所有 Winsock 2 SPI 传输服务提供者的网络协议结构和路径信息。

另外，学习中一定要有一个调试信息的监视软件。本书没有附带这样的工具，但很容易从网站上获得。例如常见的 DbgView.exe，网址是：www.sysinternals.com。也可以任意选用其他的 Debug View 工具软件。本书以 DbgView.exe 为例进行讲述。

目　录

第一部分　Windows 网络封包的截获技术

第二部分 Xfilter 个人防火墙实例剖析

第三部分 附 录

第 一 部 分

Windows 网络封包的截获技术