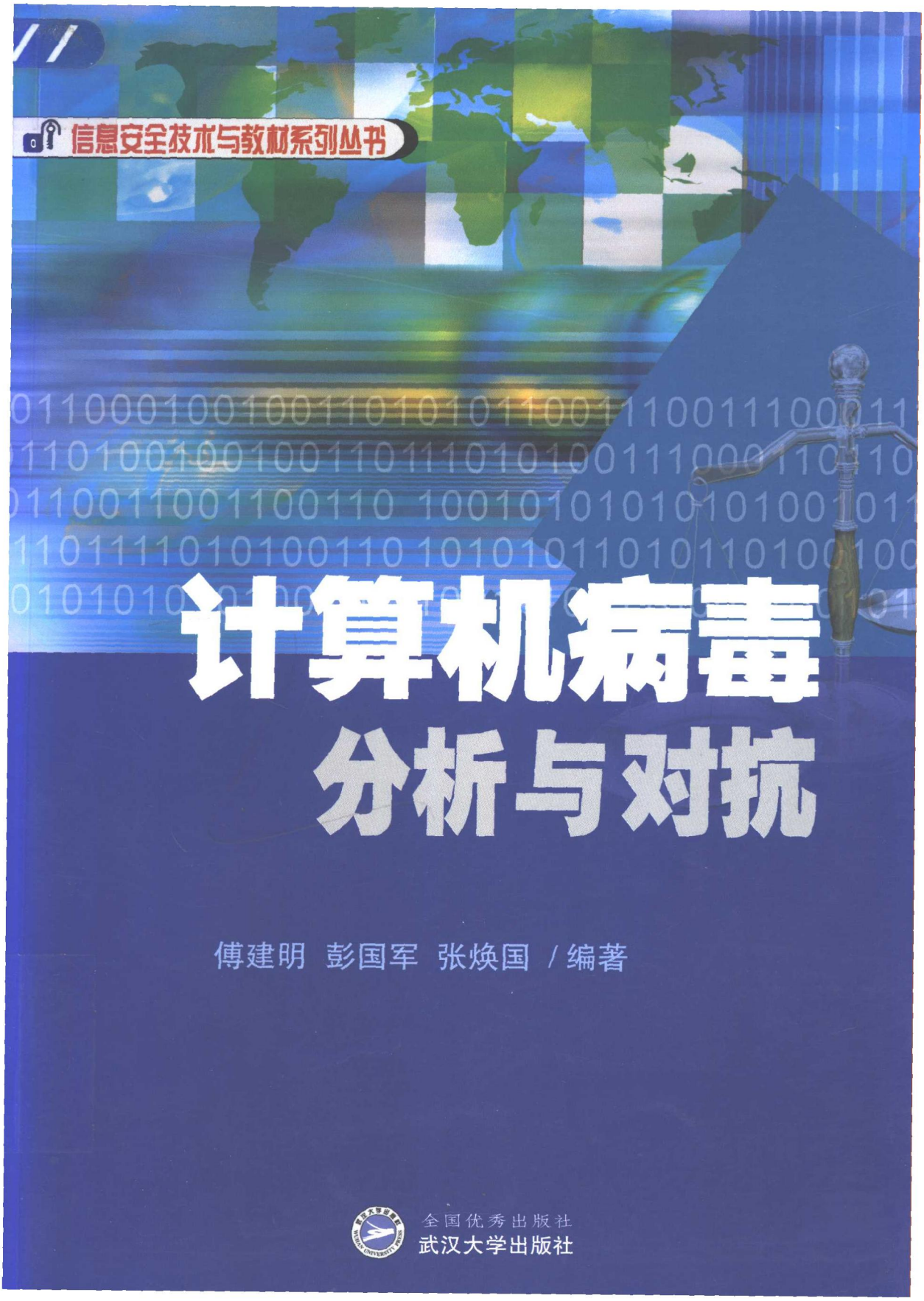
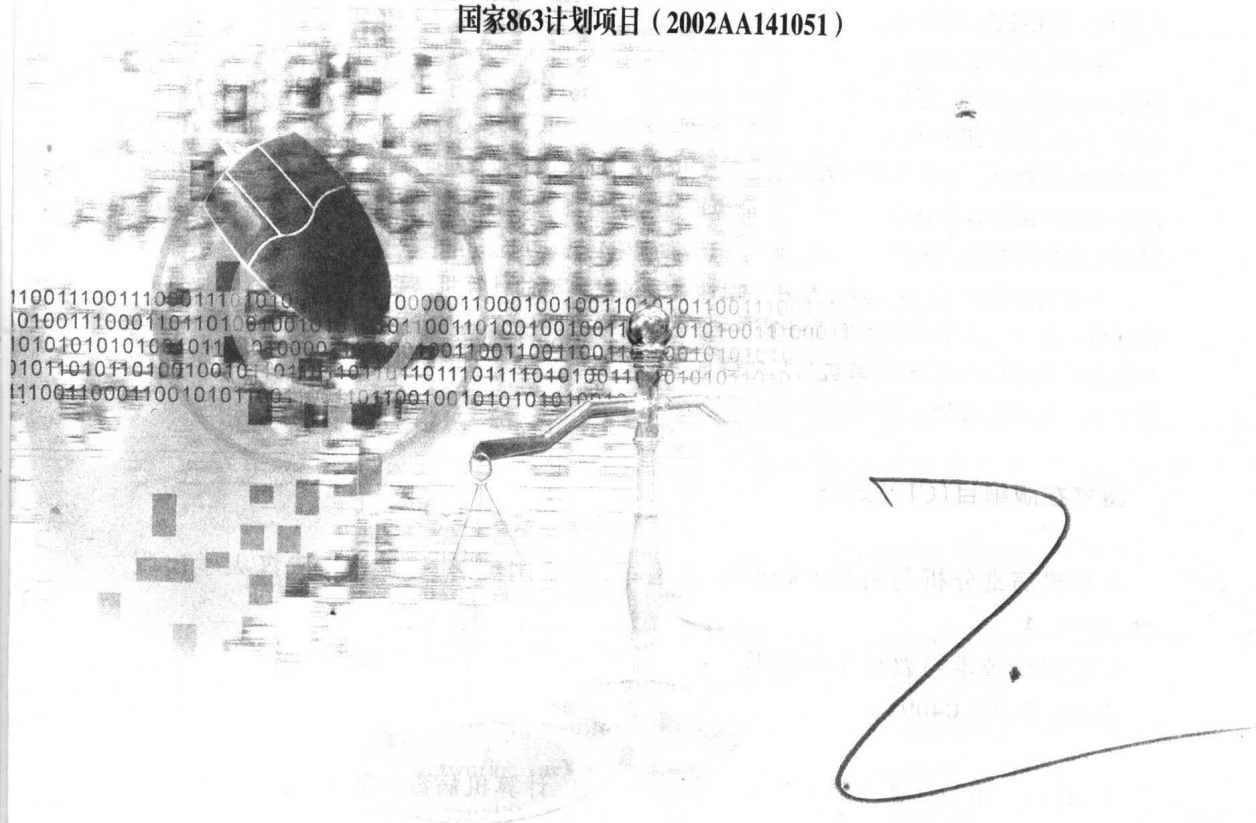

信息安全技术与教材系列丛书
计算机病毒
分析与对抗
傅建明 彭国军 张焕国 /编著
全国优秀出版社
武汉大学出版社

信息安全技术系列丛书

国家自然科学基金项目（90104005，66973034）
教育部博士点基金项目（20020486046）
国家863计划项目（2002AA141051）



计算机病毒分析与对抗

傅建明 彭国军 张焕国 /编著

全国优秀出版社
武汉大学出版社

内 容 简 介

本书比较全面地介绍了计算机病毒的基本理论和主要防治技术。特别对计算机病毒的产生机理、寄生特点、传播方式、危害表现以及防治和对抗等方面进行了比较深入的分析和探讨。

本书不仅介绍、分析了 DOS 病毒和 Windows 病毒，而且还分析了其他平台的病毒。从计算机病毒的结构、原理、源代码等方面进行了比较深入的分析，介绍了计算机病毒的自我隐藏、自加密、多态、变形、代码优化、SEH 等基本的抗分析和自我保护技术，此外还分析了木马和邮件炸弹等破坏性程序。在病毒防治技术方面，本书重点阐述了几种常见的病毒检测对抗技术，并比较详细地介绍了各类计算机病毒样本的提取过程。另外，本书也从计算机病毒的数学模型角度更深层次地对计算机病毒的特征进行了归纳和探索。

本书通俗易懂，注重可操作性和实用性。通过对典型的计算机病毒进行实例分析，使读者能够举一反三。本书可作为广大计算机用户、系统管理员、计算机安全技术人员的技术参考书，特别是可用做信息安全、计算机与其他信息学科本科学生的教材。同时，也可用做计算机信息安全职业培训的教材。

图书在版编目(CIP)数据

计算机病毒分析与对抗/傅建明，彭国军，张焕国编著.—武汉：武汉大学出版社，2004.4

信息安全技术与教材系列丛书

ISBN 7-307-04094-8

Ⅰ.计… Ⅱ.①傅… ②彭… ③张… Ⅲ.计算机病毒—防治 Ⅳ.TP309.5

中国版本图书馆 CIP 数据核字(2003)第 113367 号

责任编辑：黄金文　　**责任校对：**王　建　　**版式设计：**支　笛

出版发行：武汉大学出版社　(430072　武昌　珞珈山)

(电子邮件：wdp4@whu.edu.cn　网址：www.wdp.whu.edu.cn)

印刷：武汉大学出版社印刷总厂

开本：787×980　1/16　　印张：35.375　　字数：727 千字

版次：2004 年 4 月第 1 版　　2004 年 4 月第 1 次印刷

ISBN 7-307-04094-8/TP・147　　定价：52.00 元

信息安全技术与教材系列丛书

编委会

序　言

21世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为新的经济增长点。信息的安全保障能力成为一个国家综合国力的重要组成部分。

当前，以Internet为代表的计算机网络的迅速发展和“电子政务”、“电子商务”等信息系统的广泛应用，正引起社会和经济的深刻变革，为网络安全和信息安全开拓了新的服务空间。

世界主要工业化国家中每年因利用计算机犯罪所造成的经济损失远远超过普通经济犯罪。内外不法分子互相勾结侵害计算机系统，已成为危害计算机信息安全的普遍性、多发性事件。计算机病毒已对计算机系统的安全构成极大的威胁。社会的信息化导致新的军事革命，信息战、网络战成为新的作战形式。

总之，随着计算机在军事、政治、金融、商业等部门的广泛应用，社会对计算机的依赖越来越大，如果计算机系统的安全受到破坏将导致社会的混乱并造成巨大损失。因此，确保计算机系统的安全已成为世人关注的社会问题和计算机科学的热点研究课题。

信息安全事关国家安全，事关经济发展，必须采取措施确保信息安全。

发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。到2003年，全国设立信息安全本科专业的高等院校增加到20多所。2003年经国务院学位办批准武汉大学建立信息安全博士点。

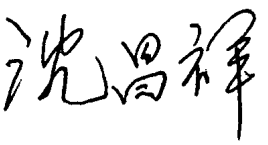
为了增进信息安全领域的学术交流、为信息安全专业的大学生提供一套适用的教材，武汉大学组织编写了这套《信息安全技术与教材系列丛书》。这套丛书涵盖了信息安全的主要专业领域，既可用做本科生的教材，又可作为工程技术人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，努力反映信息安全领域的新成果和新技术。在我国信息安全专业人才培养刚刚起步的今天，这套

丛书的出版是非常及时的和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢。欢迎广大读者提出宝贵意见，以使丛书能够进一步修改完善。

中国工程院院士，武汉大学兼职教授



前 言

随着计算机和互联网络技术的快速发展与广泛应用，计算机网络系统的安全受到严重的挑战，来自计算机病毒和黑客攻击及其他方面的威胁越来越大。其中，计算机病毒更是计算机安全中很难根治的主要威胁之一。

在日常生活中，人们大都受到过生物病毒的侵扰。人们通过与生物病毒长时间的斗争，对生物病毒已经有了比较深入的研究，从而具备了防治与对抗生物病毒的能力。

计算机和网络的普及给计算机病毒带来了前所未有的发展机会，计算机病毒给我们带来的负面影响和损失是刻骨铭心的，譬如 1999 年爆发的 CIH 病毒以及 2003 年元月的蠕虫王等都给广大用户带来了巨大的损失。因此，了解计算机病毒的原理、掌握计算机病毒的防治技术、正确认识计算机病毒，可有效地对抗计算机病毒以减少计算机病毒造成的损失。

本书从生物病毒的概念入手，介绍了计算机病毒的定义、特征、分类以及与生物病毒的联系和区别，接着阐述了计算机病毒和破坏程序的发展，其中包括计算机病毒、网络蠕虫、陷门、逻辑炸弹、拒绝服务程序和特洛伊木马等。这些内容构成了本书的第一章。希望通过本章的学习，读者能较全面了解计算机病毒等破坏性程序的基本概念和基本的预防知识。

计算机病毒涉及到较多的计算机基础知识，如操作系统、编程语言、计算机网络等。第二章从一个简单的计算机病毒的原型出发，引入计算机病毒的逻辑结构，进而介绍计算机的磁盘管理、Windows 的文件系统、计算机的引导过程、计算机的中断与异常、计算机的内存管理、EXE 文件的格式等与计算机病毒相关的预备知识。如果读者对这些知识比较熟悉，则可跳过该章。希望该章能为读者提供计算机病毒的系统知识。

在第三章中我们将计算机病毒的逻辑结构分为三部分：病毒的传播机制、触发机制和破坏机制。第三章重点阐述了计算机病毒的这三种机制，并讨论了计算机病毒的几种生存状态及它们之间的相互转换。我们知道计算机病毒的传播、触发和破坏方式是各式各样的，但是计算机病毒的传播和破坏是有它的特定条件的，了解这

些条件有利于我们把握计算机病毒的本质。

目前用户常用的操作系统大多数为 Windows 系列，少数为 DOS，Linux 等其他操作系统。由于 DOS 病毒是计算机病毒的典型代表，第四章介绍了 DOS 下的引导区病毒和文件型病毒的概述、原理和相关病毒源码分析。接着，第五章从Windows病毒出发，首先分析了 Win32 PE 病毒的原理，随后阐述了宏病毒、脚本病毒、网页病毒、网络蠕虫的原理和特征以及相关病毒的源码分析。这两章从感性上认识病毒，从原理上分析病毒，从而了解病毒的本质。

反病毒技术的不断发展迫使病毒不断地提高自己的生存能力，病毒技术得到了不断的发展。第六章分析了目前病毒常采用的抗分析技术，其中包括各种隐藏技术、花指令、简单自加密技术、多态技术、变形技术、代码优化技术、异常处理技术等。这些技术的综合运用给病毒的检测带来较大困难。

第七章介绍了木马、邮件炸弹的概念、原理以及基本的预防策略，同时也简单分析了虚假的文本文件，这些文件的运行同样也会带来很大的破坏性。本章是第四、五两章的延伸。

自第一个病毒出现后，人们通过与病毒长期的斗争，积累了大量反病毒的经验，掌握了很多实用的反病毒技术，并开发出了一些优秀的抗病毒软件产品。第八章介绍目前抗病毒软件主要采用的病毒对抗技术。本章首先阐述了特征值检测技术、校验和检测技术、行为监测技术、启发式扫描技术和虚拟机技术，接着介绍了病毒的清除和预防，最后介绍了生物免疫系统、计算机病毒免疫的原理、数字免疫系统和以毒攻毒思想。本章将进一步提高我们对反病毒技术水平的认识，这将有利于我国的反病毒事业的发展。

为了深刻认识计算机病毒的本质，人们努力用形式化的方法刻画计算机病毒。第九章介绍了计算机病毒的各种理论模型，包括基于图灵机的计算模型、基于递归函数的数学模型和互联网中蠕虫传播模型。这些模型有利于进一步深入理解计算机病毒、研究计算机病毒的各种机制。

除了前面介绍的病毒外，还有许多其他操作系统的病毒，如 UNIX/Linux 下的病毒。第十章首先概述了其他平台的病毒，然后重点介绍 UNIX/Linux 下 ELF 的文件格式以及基于 ELF 的计算机病毒原理，最后简单地介绍了手机病毒。

第十一章作为本书的结束，介绍了计算机样本的获得和提取方法，并给出了一个简单的提取实例。本章是作为前面第二章、第三章、第四章、第五章、第六章、第八章内容的实践部分。读者在提取样本时需要格外小心，因为稍有不慎会造成病毒对计算机系统的感染，甚至会造成比较严重的后果和损失。

本书第一章、第三章、第七章、第八章、第十章由傅建明和彭国军编写，第二章、第四章、第五章、第六章、第十一章由彭国军和张焕国编写，第九章由李晓丽和傅建明共同编写。全书最后由傅建明和彭国军统稿，张焕国审定。

本书的研究和编写工作受到国家自然科学基金项目（编号：6697304，90104005）、国家863计划项目（编号：2002AA141051）和教育部博士点基金项目（编号：20020486046）的资助。

本书从各种论文、书刊、期刊以及互联网中引用了大量的资料，有的在参考文献中列出，有的无法查证。在文字的录入和整理中，得到了王丽娜、周伟、程炼、杨晓东等的帮助。在此谨向他们表示衷心感谢。

由于时间和水平有限，难免有错，恳请读者批评指正，使本书得以改进和完善。

作 者

2003年6月于珞珈山

目 录