信息安全专业系列教材

计算机病毒原理与防治

Jisuanji Bingdu Yuanli yu Fangzhi

（第2版）

卓新建　郑康锋　辛　阳　编著

北京邮电大学出版社
www.buptpress.com

信息安全专业系列教材

计算机病毒原理与防治

（第2版）

卓新建　郑康锋　辛　阳　编著

北京邮电大学出版社
·北京·

内 容 简 介

计算机病毒的基本原理、防治计算机病毒的基本原理与方法是关心信息安全的人士所必须了解和掌握的内容，是信息安全研究中的重要组成部分。本书在这几个方面做了全面、系统的介绍。

第 1 章为计算机病毒的介绍；第 2 章介绍了与计算机病毒相关的操作系统知识与编程知识；第 3 章是计算机病毒原理的介绍，并分别针对 DOS、Windows、Linux 平台对传统、经典的计算机病毒的结构及运行原理进行了详细介绍；第 4～6 章分别对计算机病毒防治的 3 个方面——计算机病毒的检测、清除和预防——进行了原理分析和基本方法的介绍；第 7 章是对一些具体、经典的计算机病毒从其基本结构、运行机制到对其检测、清除或预防的综合介绍；第 8 章简要介绍了计算机病毒方面相关的法律与法规。每一章后面都配有习题以巩固相关知识，或对各章节的内容进行适当地补充。

本书可以作为高等院校信息安全、计算机、通信、信息等专业学生的教材，也可作为对计算机病毒防治有兴趣的各界人士的参考书。

图书在版编目(CIP)数据

计算机病毒原理与防治/卓新建，郑康锋，辛阳编著. —2 版. —北京：北京邮电大学出版社，2007

ISBN 978-7-5635-1422-9

Ⅰ. 计… Ⅱ. ①卓…②郑…③辛… Ⅲ. 计算机病毒—防治 Ⅳ. TP309.5

中国版本图书馆 CIP 数据核字(2007)第 119059 号

书　　名：计算机病毒原理与防治(第 2 版)
作　　者：卓新建　郑康锋　辛阳
责任编辑：李欣一
出版发行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
北方营销中心：电话：010-62282185　传真：010-62283578
南方营销中心：电话：010-62282902　传真：010-62282735
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京源海印刷有限责任公司
开　　本：787 mm×960 mm　1/16
印　　张：21.5
字　　数：468 千字
印　　数：1—5 000 册
版　　次：2004 年 4 月第 1 版　2007 年 8 月第 2 版　2007 年 8 月第 1 次印刷

ISBN 978-7-5635-1422-9/TP・285　　定　价：32.00 元

信息安全专业系列教材（第2版）

编 委 会

第2版总序

发展21世纪中国信息安全要靠教育，而搞好信息安全教育就需要好的教材。2004年，北京邮电大学信息安全中心完成了第一套信息安全专业本科系列教材，该套教材被评为“北京市高等教育精品教材立项项目”，而后又被教育部列入“普通高等教育‘十五’国家级规划教材”。至今，三年多的时间过去了，这套教材在信息安全专业的教学中发挥了重要的作用，起到了较好的教学效果，受到教师和学生的好评。

在这三年中，我们始终致力于包括专业建设、课程建设、师资建设、教材建设、实训基地建设、实验室建设及校企就业（创业）平台建设等在内的信息安全本科专业的全面建设。2005年，作为组长单位，我们完成了教育部“信息安全专业规范研究”和“信息安全学科专业发展战略研究”课题；召开了“全国高校本科‘信息安全专业规范与发展战略研究’成果发布与研讨会”；在国内第一次制定了信息安全专业规范，从知识领域、知识单元和知识点三个层次构建学科专业教学的知识体系；由通识教育内容、专业教育内容和综合教育内容三大部分构建课程参考体系；采用顶层设计的方法构建了带有实践性环节的教学体系；在国内第一次较全面地提出信息安全学科专业教学改革与创新研究的发展思路和政策建议，成果提交教育部教学指导委员会，对于引导高等学校信息安全学科专业教学改革与建设，指导信息安全学科专业评估，促进信息安全学科专业教学规范建设与管理，提高专业教育质量和水平有重要的作用。多所举办信息安全专业的高校都参照课题成果调整了自己的教学计划、课程体系和实验方案。

积极搭建信息安全专业校际交流平台。组织成立了“全国信息安全本科教材编写委员会”和“全国信息安全本科专业师资交流与培训互助组”。主持召开了“全国信息安全专业教学经验交流和师资培训研讨会”及“全国信息安全专业实验室建设和实验课程教学经验交流研讨会”。在四川绵阳建设了占地两万六千多平方米的全国信息安全专业本科生实习实训基地，接收了来自全国近30所高校的本科生进入该基地参加丰富多彩的实训。

努力建设精品课程。召开了“全国高校信息安全专业精品课程建设经验交流会议”，来自全国各地高校的专家齐聚北邮，介绍与交流了精品课程建设的经验。组织建设了全国第一批信息安全实验室，并且编写出版了信息安全实验指导教材，2007年，我们的《现代密码学》课程申报了北京市精品课程，已经被专家评审通过，目前正在申报2007年度“国家精品课程”。

三年多的时间过去了，信息安全的教育和产业都取得了丰硕的成果，随着信息安全向更高层次的发展，其趋势已经从基础的网络层建设开始向内容层建设过渡。为适应信息安全教育的发展需要，积极探索培养创新型高素质人才，我们按照制定的学科发展战略和专业规范的精神，结合近几年的教学实践，对原信息安全专业本科系列教材进行了全面修订。这次修订不仅对原来的系列教材在第1版的基础上进行修改和完善，还补充了信息安全最新的研究成果，使教材的内容更加翔实和新颖。同时，在原有体系的基础上又增加了一些新的课程教材。在新修订的系列教材中，目前有《信息安全概论(第2版)》、《现代密码学及其应用》、《网络安全(第2版)》、《信息安全管理》、《计算机病毒原理与防治(第2版)》、《数字版权管理》、《计算机系统安全》、《网络安全实验教程》、《信息安全专业科技英语》、《防火墙、入侵检测与VPN》、《对称密码学及其应用》、《信息安全导论》等12本教材。随着信息安全专业教学的需要，今后还将不断有新的教材补充进来。希望通过对内容的精心组织和设计能促进信息安全课程的建设，同时涌现出更多的信息安全精品课程。

在这次修订中，我们组织了强大的师资队伍，将多次讲授相关课程的教师充实到本次修订队伍中。经过反复研讨，本着理论与实际相结合的原则，对原来的系列教材进行了较大的修改和扩充，我们希望这套新修订的系列教材能够满足国内各类高校信息安全本科专业以及相关方向的不同需求。

虽然我们在这次修订中投入了很大精力，但是由于水平有限，时间仓促，且信息安全专业的发展速度非常快，不足之处和错误在所难免，我们衷心期望使用和关心该系列教材的师生，继续对新的系列教材提出宝贵意见和建议。

本系列教材也是国家重点基础研究发展计划(973)(课题编号：2007CB310704和2007CB311203)资助的成果，并在积极申报“普通高等教育‘十一五’国家级规划教材”。

在本系列教材的修订过程中，得到了北京邮电大学出版社的大力支持，同时也得到了北京邮电大学信息安全中心成员的支持与配合，在此一并表示感谢。

教授、博士生导师、全国政协委员

杨义先

前　言

目前，信息安全已经成为研究的热点，而计算机病毒则是信息安全研究的重要内容之一，对该方向的人才需求也相应地快速增长，全国各大高校相继设立了信息安全专业以适应培养信息安全专业人才的需求。

北京邮电大学信息工程学院较早在全国开设了信息安全本科专业，并在信息安全专家杨义先教授和温巧燕教授的组织下，编写了信息安全专业系列教材，并被列为“普通高等教育‘十五’国家级规划教材”。本书的第 1 版《计算机病毒原理与防治》即为该系列教材之一。

本书第 1 版系统、全面地介绍了计算机病毒的基本原理以及防治计算机病毒的基本原理及基本方法，主要以 DOS 操作系统为主线进行计算机病毒的原理介绍和实例讲解。随着 Windows 及 Linux 等操作系统的普及，针对计算机病毒的研究已经从 DOS 平台转化到 Windows 及 Linux 平台。因此，本书在第 1 版的基础上增加了 Windows 及 Linux 操作系统下计算机病毒的原理与实例，并对 Windows 及 Linux 操作系统基础、编程知识以及一些主流的工具软件进行了简单介绍，还增加了相关法律法规等内容。

本书共有 8 章，主要内容为计算机病毒的基本原理以及防治计算机病毒的基本原理及基本方法。每章内容简介如下。

第 1 章为计算机病毒的介绍，主要包括计算机病毒的定义、基本特征及分类，作者特别在参阅了大量资料之后，编写了计算机病毒的发展简史，以及计算机病毒在我国的发展简况；之后对计算机病毒的产生及相关社会问题进行了分析，最后简述了计算机病毒防治的基本方法。

第 2 章为与计算机病毒相关的操作系统知识与编程知识，这是了解计算机病毒原理的基础。

第 3 章为计算机病毒原理的介绍，分别针对 DOS、Windows、Linux 平台对传统、经典的计算机病毒的结构及运行原理进行了详细介绍，并对当前流行的网络、脚本病毒进行了跟踪解释和分析，最后还对新一代病毒的特点及计算机病毒的发展趋势进行了探讨。

第 4～6 章分别对计算机病毒防治的 3 个方面——计算机病毒的检测、清除和预

防——进行了原理分析和基本方法的介绍。

第 7 章综合介绍一些具体、经典的计算机病毒的基本结构、运行机制及对其检测、清除或预防的方法。

第 8 章简要介绍了计算机病毒方面相关的法律法规。

本书的编写得到了北京邮电大学信息工程学院博士研究生李基，硕士研究生金狄、郭航、代闻、贺卉珍等同学的很多帮助，作者在此表示衷心的感谢，他们与作者对计算机病毒分析、计算机病毒防治等各方面的讨论、分析使作者受益匪浅。

由于作者水平所限，本书问题和不足之处在所难免，恳请广大读者批评指正。

作　者

目　录

第 3 章 计算机病毒的结构及作用机制

第 4 章 检测计算机病毒的基本方法

第1章

计算机病毒的基础知识及发展简史

计算机技术的迅猛发展，给人们的工作和生活带来了前所未有的便利和效率，随着计算机走进社会的各个领域，走进千家万户，计算机系统已能实现对工作、生活、管理、办公的自动化，成为人类社会不可缺少的一部分。与此同时，计算机安全的重要性也被越来越多的人认识到，商业界、金融银行界要依靠计算机处理事务；政府的行政管理要依靠计算机信息系统和数据库；厂家和公司的全部生产取决于数据处理系统的能力；陆海空、宇航等指挥控制系统，医疗卫生要依靠计算机技术；整个社会对计算机信息系统的依赖程度越来越大，甚至离不开它。然而，计算机系统并不安全，其不安全因素有计算机信息系统自身的、自然的，也有人为的。

计算机病毒就是最不安全的因素之一。计算机病毒是现代信息化社会的公害，是计算机犯罪的一种特殊形式。各种计算机病毒的产生和全球性蔓延已经给计算机系统的安全造成了巨大的威胁和损害，其造成的计算机资源的损失和破坏，不但会造成资源和财富的巨大浪费，而且有可能造成社会性的灾难，正由于此，人们开始了反计算机病毒的研究。随着信息化社会的发展，计算机病毒的威胁日益严重，迄今为止，已发现的计算机病毒种类很多，且以相当惊人的速度递增，令人们谈病毒而色变。人们将计算机病毒称之为“21世纪最大的隐患”、“不流血的致命武器”，它的出现完全有可能改变人类的未来，因此反病毒的任务更加艰巨了。

随着计算机网络的发展，计算机病毒对信息安全的威胁日益严重，我们一方面要掌握对当前计算机病毒的防范措施，另一方面要加强对病毒未来发展趋势的研究，真正做到防患于未然。我们要提前做好技术上的储备，严阵以待，保障信息安全。为使人们对计算机病毒有更多的理解，以便有效地预防和清除病毒，本书采用理论与实例结合的方法，介绍计算机病毒的基本常识和计算机病毒的机制，以及防治计算机病毒的方法和典型计算机病毒的预防技术。

1.1 计算机病毒的定义

计算机病毒是一个程序，一段可执行码。像生物病毒一样，计算机病毒有其独特的复制能力，可以很快地蔓延，又常常难以根除，它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。现在，随着计算机网络的发展，计算机病毒和计算机网络技术相结合，蔓延得更加迅速。

在生物学中，病毒是指侵入动植物体等有机生命体中的具有感染性、潜伏性、破坏性的微生物，而且不同的病毒具有不同的诱发因素。“计算机病毒”一词是人们联系到破坏计算机系统的“病原体”具有与生物病毒相似的特征，借用生物学病毒而使用的计算机术语。“计算机病毒”一词最早出现在美国作家 Thomas J. Ryan 于 1977 年出版的科幻小说《The Adolescence of P-1》(P-1 的青春)中。

1983 年，美国计算机安全专家 Frederick Cohen 博士首次提出计算机病毒的存在，他认为：计算机病毒是一个能感染其他程序的程序，它靠修改其他程序，并把自身的复件嵌入其他程序而实现病毒的感染。1989 年，他进一步将计算机病毒定义为：“病毒程序通过修改其他程序的方法将自己的精确复件或可能演化的形式放入其他程序中，从而感染它们。”所谓感染，是指病毒将自身嵌入到指令序列中，致使执行合法程序的操作招致病毒程序的共同执行(或是以病毒程序的执行取而代之)。

1994 年《中华人们共和国计算机安全保护条例》定义：“计算机病毒是指编制或者在计算机程序中插入的，破坏计算机功能或数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。”

当然，还有其他人的不完全相同的定义，但都大同小异。从广义上说，凡是能引起计算机故障、破坏计算机数据的程序统称为计算机病毒。近年来，各种恶意代码之间的界限有模糊的趋势，人们不再刻意地区分是计算机病毒、网络蠕虫，还是木马、僵尸网络等。但在本书中，还是会将这些恶意代码的概念进行一些区别介绍，以使读者更好地理解计算机病毒。

1.2 病毒的基本特征

计算机病毒是一段特殊的程序，它与生物学病毒有着十分相似的特性。除了与其他程序一样，可以存储和运行外，计算机病毒(简称病毒)还有感染性、潜伏性、可触发性、破坏性、衍生性等特征。它一般都隐蔽在合法程序(被感染的合法程序被称为宿主程序)中，当计算机运行时，它与合法的程序争夺系统的控制权，从而对计算机系统实施干扰和破坏作用。

病毒程序与正常程序的区别：①正常程序是具有应用功能的完整程序，以文件形式存在，具有合法文件名；而病毒一般不以文件的形式独立存在，一般没有文件名，它隐藏在正

常程序和数据文件中，是一种非完整的程序；②正常程序依照用户的命令执行，完全在用户的意愿下完成某种操作，也不会自身复制；而病毒在用户完全不知的情况下运行，将自身复制到其他正常程序中，而且与合法程序争夺系统的控制权，甚至进行各种破坏。

1. 感染性

计算机病毒的感染性也称为寄生性，指计算机病毒程序嵌入到宿主程序中，依赖于宿主程序的执行而生存的特性。感染性是计算机病毒的根本属性，是判断一个程序是否为病毒程序的主要依据。病毒可以感染文件、磁盘、个人计算机、局部网络、互联网，病毒的感染是指从一个网络侵入另一个网络，由一个系统扩散到另一个系统，由一个系统传入到另一个磁盘，由一个磁盘进入到另一个磁盘，或者由一个文件传播到另一个文件的过程。以前，软盘和光盘是计算机病毒的主要感染载体；现在，网络（主要包括电子邮件、BBS、WWW 浏览、FTP 文件下载等）成了计算机病毒最主要的感染载体；点对点的通信系统和无线通信系统则是最新出现的病毒的感染载体。

感染性是病毒的再生机制，病毒通过修改磁盘扇区信息或文件内容，并与系统中的宿主程序链接在一起达到感染的目的，继而它就会在运行这一被感染的程序之后开始感染其他程序，这样一来，病毒就会很快地感染到整个系统。一个感染上病毒的计算机系统同样具有破坏性。

病毒的感染性与计算机系统的兼容性有关，或者说计算机病毒一般都是针对某一种或几种计算机和特定的操作系统进行攻击的。目前世界上出现的病毒都不能对所有的计算机系统进行感染。例如，有的针对 PC 机及其兼容机，有的针对苹果公司 Macintosh 系列机，也有的针对 Unix 或 Linux 操作系统，有的针对微软的操作系统，有的专门针对网络，也有的能同时感染网络和操作系统，如 2001 年 9 月出现的 Nimda 病毒（但也只是针对某些特定的操作系统）。只有一种计算机病毒几乎是与操作系统无关的，那就是宏病毒，所有能够运行 Office 文档的地方都可能有宏病毒的存在。

2. 隐藏性

隐藏性是计算机病毒的基本特征之一。

从病毒隐藏的位置来看，有些病毒将自己隐藏在磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中；也有个别的病毒以隐藏文件的形式出现；还有一种比较常见的隐藏方式是将病毒文件放在 Windows 等系统的系统目录下，并将文件命名为类似 Windows 等系统的系统文件的名称，使对计算机操作系统不熟悉的人不敢轻易删除它。

不同类型的病毒采用的隐藏技术不同。有些病毒感染正常程序时将程序文件压缩，留出空间嵌入病毒程序，这样使被感染病毒的程序文件的长度变化很小，很难被发现。还有些病毒可以加密、变型（多态病毒）或防止反汇编、防跟踪等，都是为了不让被感染的计算机用户发现。

计算机病毒的隐藏性表现在两个方面。

（1）感染的隐藏性。大多数病毒的代码设计得非常精巧而短小，一般只有几百字节或几千字节，而 PC 机对文件的存取速度可达每秒几兆字节以上，所以病毒转瞬之间便可

将这短短的几百字节附着到正常程序之中，且一般不会有外部表现，从而不易被人发现。

（2）病毒程序存在的隐藏性。病毒通常以隐藏的方式存在，这又包括了在潜伏期的隐藏和触发后的隐藏。正常程序被计算机病毒感染后，其原有功能基本上不受影响，病毒代码附于其上而得以存活并不断地得到运行的机会，从而进行进一步的传播，生成更多的复制体，与正常程序争夺系统的控制权和系统资源，不断地破坏系统。

3. 潜伏性

病毒的潜伏性是指其具有依附于其他媒体而寄生的能力，即通过修改其他程序而把自身的复制体嵌入到其他程序或磁盘的引导区（包括硬盘的主引导区）中寄生。当计算机病毒侵入系统后，其触发是由触发条件来确定的。在触发条件满足前，病毒具有一定的潜伏期，可以在系统中没有表现症状，从而不影响系统的正常运行。一旦条件满足，病毒就会不断地进行感染。一个编制巧妙的计算机病毒程序可以在一段很长的时间内隐藏在合法程序中，对其他系统进行感染而不被人们发现。病毒的潜伏性与感染性相辅相承，潜伏性越好，它在系统中存在的时间就会越长，病毒的感染范围也就越大。

4. 可触发性

病毒一般都有一个触发条件：或者触发其感染，即在一定的条件下激活一个病毒的感染机制使之进行感染；或者触发其发作，即在一定条件下激活病毒的表现（破坏）部分。条件判断是病毒自身特有的功能，一种病毒一般设置一定的触发条件。病毒程序在运行时，每次都要检测控制条件，一旦条件成熟，病毒就开始感染或发作。触发条件可能是指定的某个时间或日期、特定的用户识别符的出现、特定文件的出现或使用次数、用户的安全保密等级、某些特定的数据等。

5. 衍生性

计算机病毒的制造者可以依据个人的主观愿望，对某一个已知病毒程序做出修改而衍生出另外一种或多种“来源于同一种病毒，而又不同于源病毒程序的病毒程序”，通常把这样一类程序称为源病毒程序的变种，这就是计算机病毒的衍生性。有些病毒可以产生几十种甚至上百种变种，这种衍生性可以是人为的结构，也可以是“计算机病毒自动生成”这种人工智能的结果。变种可能与源病毒有很相似的特征；如果衍生的计算机病毒已经与以前的计算机病毒有了很大甚至是根本性的差别，就会将其认为是一种新的计算机病毒。变种或新的计算机病毒可能比原计算机病毒有更大的危害性。变种病毒可以在一定程度上躲避查杀病毒软件，从而增强病毒的生命力。

6. 破坏性

计算机病毒的破坏性取决于病毒设计者的目的和水平。如果病毒设计者的目的在于破坏系统的正常运行，则可以毁掉或修改系统内的部分或全部数据或文件，例如改写文件、删除文件、格式化磁盘等；可以干扰或迷惑用户的操作，例如锁死键盘或修改键盘的功能等；可以干扰系统的运行，如干扰屏幕显示、降低机器的运行速度等；也可以损坏硬件（主板、磁盘等）。即使有的病毒只是为了表现自己而不进行破坏活动，比如有的病毒可能

只是显示一串无用甚至“有趣”的提示信息，甚至还有极少数病毒被有些人称为“好病毒”（有一个病毒可以对文件进行自动压缩，好像可以节约磁盘空间），但也降低了计算机系统的工作效率，并干扰或违背了用户的意愿，更重要的是有时本没有多大破坏作用的病毒的重复感染或几种病毒交叉感染或并行感染，也会导致文件、系统崩溃等重大恶果。所以正常用户一旦发现计算机病毒，最好立即清除，而恶意制造计算机病毒的行为必须被制止或受到惩罚，所谓的“好意”也要慎之又慎，而且要对所引起的一切后果负责。

归纳起来，计算机病毒的危害大致有如下几个方面。

（1）对计算机数据信息的直接破坏作用

直接破坏作用主要包括攻击系统数据区，攻击部位包括：硬盘主引导扇区、引导扇区、FAT表、文件目录区。攻击文件时，攻击方式可列举如下：删除、改名、替换内容、丢失部分程序代码、内容颠倒、写入时间空白、变碎片、假冒文件、丢失文件簇、丢失数据文件等及格式化磁盘。

（2）抢占系统资源

占用和消耗系统的内存资源或禁止分配内存、改变中断等；干扰系统运行（如不执行命令、干扰内部命令的执行、虚假报警、打不开文件、内部栈溢出、占用特殊数据区、换现行盘、时钟倒转、重启动、死机、强制游戏、扰乱串并行口）；攻击磁盘数据、不写盘、写操作变读操作、写盘时丢字节、抢占磁盘空间；扰乱屏幕显示，干扰键盘操作，干扰喇叭、打印机等I/O设备的正常工作；破坏CMOS设置（在机器的CMOS区中，保存着系统的重要数据，如系统时钟、磁盘类型、内存容量、校验和等。有的病毒能对CMOS区进行写入动作，破坏系统CMOS中的数据）等。

（3）影响计算机运行速度

计算机病毒程序为了运行自己的程序，抢占系统资源，必然影响计算机的运行速度，甚至有的病毒在时钟中纳入了时间的循环计数，迫使计算机空转，使计算机速度明显下降。

（4）病毒对计算机硬件的破坏

以前的各种病毒最多只能破坏硬盘数据，CIH病毒却能侵入主板上的Flash BIOS，破坏其内容而使主板报废。现在还有以下一些计算机的硬件已经或很容易遭到计算机病毒的破坏：显示器，每台显示器都有自己的带宽和最高分辨率、场频，若其中有一项超过，就会出现花屏，严重了就会烧坏显示器，病毒可以通过篡改显示参数来破坏显示器（如把分辨率、场频改到显卡能支持的最高挡等）；支持“软跳线”的主板、CPU、显卡、内存等，目前新型主板采用“软跳线”的越来越多，这正好给病毒以可乘之机（所谓“软跳线”是指在BIOS中就能改动CPU的电压、外频和倍频），病毒可以通过改BIOS参数，加高CPU电压使其过热而烧坏，或提高CPU的外频，使CPU和显卡、内存等外设超负荷工作而过热烧坏，有些显卡也可通过改变其芯片的频率使其超负荷工作而烧坏。此外病毒还可使光驱、硬盘、打印机等设备超负荷工作而大大缩短使用寿命。