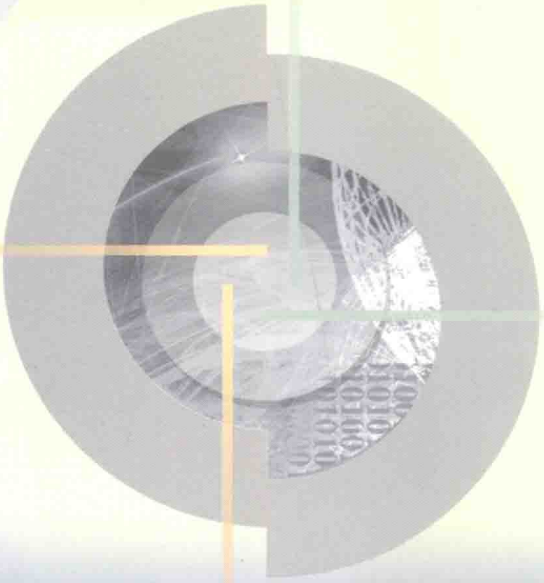
普通高等教育“十五”国家级规划教材

信息安全专业系列教材

北京市高等教育精品教材立项项目

计算机病毒原理及防治

JISUANJI BINGDU YUANLI JI FANGZHI



卓新建　主编

北京邮电大学出版社
www.buptpress.com

普通高等教育“十五”国家级规划教材

计算机病毒原理及防治

卓新建　主编

北京邮电大学出版社
·北京·

内 容 简 介

计算机病毒的防治是信息安全中非常重要的一个方面，计算机病毒的基本原理和计算机病毒防治的基本原理及基本方法都是关心信息安全方面的人士所必须了解和掌握的基本内容。本书在这几个方面作了全面系统的介绍。

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DOS基本系统知识；第3章为计算机病毒原理的介绍；第4～6章分别对计算机病毒防治的三个方面：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章是对一些具体的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。每章后面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

计算机病毒原理及防治/卓新建主编. —北京：北京邮电大学出版社，2004
ISBN 7-5635-0650-0

Ⅰ.计… Ⅱ.卓… Ⅲ.①计算机病毒—理论②计算机病毒—防治 Ⅳ.TP309.5

中国版本图书馆CIP数据核字(2004)第025252号

书　　名：计算机病毒原理及防治
主　　编：卓新建
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(100876)
电话传真：010-62282185(发行部) 010-62283578(FAX)
电子信箱：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×1 092 mm　1/16
印　　张：15
字　　数：326千字
印　　数：1—5 000册
版　　次：2004年4月第1版　2004年4月第1次印刷

ISBN 7-5635-0650-0/TP·82　　定　价：25.00元

信息安全专业系列教材

编　委　会

总　序

办好信息安全本科专业的第一要素是拥有高质量的教材。由于各方面的原因，我国开办信息安全本科专业的历史很短，刚刚起步，但是，当前以各种形式开办信息安全本科专业的高等院校却非常多，学生总数也相当可观，而且其中大部分学生已经学完基础课程，即将进入专业课的学习阶段。

与信息安全本科专业招生的火爆场面形成鲜明对比的是，到目前为止，我国还没有一套自己的信息安全本科专业系列教材。为了保证信息安全本科专业学生的培养质量，2001 年，北京市教委以“精品教材立项”的形式委托我们北京邮电大学信息安全中心负责编写《现代密码学基础》、《信息安全概论》、《网络安全》、《信息隐藏与数字水印》、《入侵检测》、《计算机病毒原理及防治》等 6 本教材，随后，教育部又将此套系列教材列入了“普通高等教育‘十五’国家级教材规划”。由此可见，此套教材的编写确实受到了各级教育主管部门的高度重视。

北京邮电大学信息安全中心是一专门从事信息安全的教学、科研和成果转化的重点实验室。该实验室已经培养出了我国第一位密码学博士，而且在“信息安全”和“密码学”两个专业领域内健全了博士后、博士、硕士和本科的培养教育体系，已经培养出了数以百计的信息安全研究生。

在接受了北京市教委和教育部的编写信息安全本科系列教材的任务之后，我们立即组织了最强的师资队伍投入到教材的编写工作之中。经过两年多的不懈努力，数易其稿，反复研讨，按照教育目标和大学生基本素质培养的要求，本着推进理工融合及学科交叉的思想，经过优化课程体系和精选课程内容，我们终于完成了信息安全本科专业系列教材的第一批教材（共 6 本）。现在我们正在着手规划信息安全本科专业的第二批教材，它们的暂定名分别是《安全操作系统》、《安全数据库》、《安全访问控制》、《安全检测与监控》、《数字证书与管理》、《安全备份与灾难恢复》、《安全隔离技术》、《安全服务技术》、《安

全系统工程》、《安全规范与标准》等。我们诚意邀请国内所有高等院校的权威安全专家加入第二批教材的编写工作(有意者请与我们直接联系。地址:100876,北京邮电大学信息安全中心126信箱)。我们希望这套信息安全本科专业系列教材最终完成之后能够基本满足国内各类高校信息安全本科专业的普遍需求。

虽然我们的目标是编写一套适合信息安全专业本科生使用的精品教材,但是,由于水平有限,时间仓促,且信息安全本科专业刚刚开始,我们还没有足够的实践机会,不足之处和错误在所难免,恳请读者和同行专家多提意见,以便我们再版时充分修改,不断完善。

衷心感谢北京邮电大学胡正名教授对本套教材的大力支持,感谢北京邮电大学信息安全中心二百余位成员的支持与配合。本套教材也是国家自然科学基金项目(90204017, 60372094, 60373059)和国家"973"项目(G1999035804)资助的成果,在此一并表示感谢。

杨义先 教授、博士生导师、全国政协委员

2004年1月于北京邮电大学信息安全中心

前　言

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，而目前全国只是有一些相关的研究专著或面向普通大众的介绍性读本或文章，而缺乏适用于信息安全本科专业的专用教材。在这种情况下，北京邮电大学在信息安全专家杨义先教授和温巧燕教授的组织下，申请了北京市高等教育精品教材建设立项——信息安全专业系列教材，目的就是专门编写一套适合信息安全专业的本科生学习或研究的精品教材。本书正是此系列教材中计算机病毒原理及防治方面的一本。

计算机病毒防治是信息安全中非常重要的一个方面，计算机病毒也是引出信息安全问题的根本原因之一，所以计算机病毒的基本原理和计算机病毒防治的基本原理及基本方法都是信息安全专业的学生必须了解和掌握的基本内容。当然本书也适合其他专业对信息安全有兴趣的本科生或硕士生学习或研究。

本书共有7章，主要内容为计算机病毒的基本原理介绍和计算机病毒防治的基本原理和基本方法。逐章内容简介如下：

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、分类，特别是在参阅了大量资料之后，编出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章内容为与计算机病毒相关的DOS基本系统知识，这是了解计算机病毒原理和计算机病毒防治的基础。第3章是计算机病毒原理的介绍，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三个方面：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。

本书的编写得到了北京邮电大学信息工程学院研究生韩杰，本科生秦臻、刘嘉、张泉、胡光耀等同学的很多帮助，作者在此表示衷心的感谢，他们在部分文字录入和资料收集方面，以及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。

最后作者对本书引用到的文献或一些资料的作者表示衷心的感谢。

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

2004 年 3 月

目　录

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，已发现的病毒种类很多，且还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，保障我们的信息安全。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，本书将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，蔓延的速度更加迅速。

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》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，并把自身的拷贝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拷贝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。

1.2 计算机病毒的基本特征

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（被感染的合法程序称作宿主程序）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。

1. 感染性

计算机病毒的感染性是指计算机病毒具有把自身复制到其他程序中的特性。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 Apple 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，如最近出现的 Nimuda 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．潜伏性（隐藏性）

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品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。这种繁殖的能力是隐蔽的，病毒的感染过程一般都不带有外部表现，大多数病毒的感染速度极快。而且大多数病毒都采用特殊的隐藏技术，例如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，这样使被病毒感染的程序文件的长度变化很小，很难被发现；有些病毒修改文件的属性等；还有些病毒可以加密、变型（多态病毒）或防止反汇编、防跟踪等等都是为了不让被感染的计算机用户发现。当计算机病毒侵入系统后，一般并不立即发作，而是具有一定的潜伏期。在潜伏期，只要条件许可，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成，潜伏性越好，其在系统中存在的时间就会越长，病毒的感染范围也就越大。

3．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、某些特定的数据等等。

4．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作"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

主要包括攻击系统数据区,攻击部位包括:硬盘主引导扇区、BOOT 扇区、FAT、文件目录区;攻击文件,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、丢失数据文件等等;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,若其中有一项超标,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档等);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。

(5) 衍生性

既然计算机病毒是一段特殊的程序，了解病毒程序的人就可以根据其个人意图随意改动，从而衍生出另一种不同于原版病毒的新病毒，这种衍生出的病毒可能与原先的计算机病毒有很相似的特征，所以被称为原病毒的一个变种；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，则此时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。

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。

1.3 计算机病毒的分类

目前，病毒到底有多少，各种说法不一。2000 年 12 月在日本东京举行的“亚洲计算机反病毒大会”的报告中说，2000 年 11 月以前的病毒数量超过 55000 种；目前，有的防病毒销售商则声称收集了 60000 种左右的 PC 病毒(有些声明是骗人的)；WildList Organization 在 2001 年 7 月的报告中列出了 698 种，但 SupplementalList 连同 WildList Proper 只列出了 214 种。谁更准确呢？除去某些哗众取宠的因素，如何定义不同的病毒也是造成这种统计区别的一个重要因素。比如有人按照“两个病毒在它们连续的代码和数据范围内，即使只有一个比特的区别也是不同的”的定义，病毒的数量自然会很大，因为这样来看，一个病毒生产机生产出的各种大同小异的病毒都是不同的，各种病毒的变种当然也是不同的。

但不管怎样，病毒的数量确实在不断地增加，而且它们种类不一，感染目标和破坏行为也不尽相同。对病毒进行分类是为了更好地了解它们。

1.3.1 传统计算机病毒

按照计算机病毒的诸多特点及特性，其分类方法有很多种，同一种病毒按照不同的分类方法可能被分到许多不同的类别中。大致有如下几种不同的分类方法：

1. 按计算机病毒攻击的机型分类

(1) 攻击微型机的病毒

微型机可以说是世界上使用最多的计算机类型，目前超过几亿台，这些机器广泛渗透到各个国家的政治、军事、经济以及人们日常生活的各个方面。而病毒的设计者总是希望病毒的传播范围越广越好，所以，这类病毒出现的最多，其变种也最多，版本的更新也最