特色专业

普通高等教育信息安全类国家级特色专业系列规划教材

计算机病毒原理及防范技术

秦志光　张凤荔　刘　峤　编著
马建峰　主审

科学出版社

内 容 简 介

本书主要内容包括计算机病毒概述、计算机病毒的工作机制、计算机病毒的表现、新型计算机病毒的发展趋势、计算机病毒检测技术、典型病毒的防范技术、网络安全、即时通信病毒和移动通信病毒分析、操作系统漏洞攻击和网络钓鱼概述、常用反病毒软件等。

本书内容丰富，具有先进性和实用性，既是一本计算机病毒与技术的专著，也是一本计算机病毒与防范技术的教材。

本书可作为信息安全、计算机，以及各类信息技术、管理学等专业的大学本科生和硕士研究生的教材或参考书，也可作为从事计算机病毒研究和应用工程开发的科技、管理、工程人员的参考书。

图书在版编目(CIP)数据

计算机病毒原理及防范技术/秦志光，张凤荔，刘峤编著. —北京：科学出版社，2012
（普通高等教育信息安全类国家级特色专业系列规划教材）
ISBN 978-7-03-034432-8

Ⅰ.①计… Ⅱ.①秦…②张…③刘… Ⅲ.①计算机病毒-防治-高等学校-教材 Ⅳ.①TP309.5

中国版本图书馆 CIP 数据核字(2012)第 105928 号

丛书策划：匡 敏 潘斯斯
责任编辑：潘斯斯 张丽花 / 责任校对：林青梅
责任印制：闫 磊 / 封面设计：迷底书装

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

化学工业出版社印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2012 年 6 月第 一 版 开本：787×1092 1/16
2012 年 6 月第一次印刷 印张：16 3/4
字数：438 000

定价：35.00 元

（如有印装质量问题，我社负责调换）

丛书序

当今社会，信息已经成为最具活力的生产要素和重要战略资源。信息技术改变着人们的生活和工作方式。信息产业已成为世界第一大产业。信息的获取、处理和安全保障能力成为综合国力的重要组成部分，信息安全已成为影响国家安全、社会稳定和经济发展的决定性因素之一。

目前关于信息安全的定义和内涵，尚未形成一个统一的说法。不同的学者给出了不同的诠释。尽管这些诠释不尽相同，但是其主要内容却是相同的。我们应当从信息系统角度来全面诠释信息安全的内涵。

信息安全学科是综合计算机、电子、通信、数学、物理、生物、管理、法律、教育等学科演绎而成的交叉学科，它与这些学科既有紧密的联系和渊源，又具有本质的不同，从而构成一门独立的学科。

随着学科的交叉发展和产业的整合，各专业方向已彼此渗透交融。如何拓宽专业方向？如何体现专业特色？是当前我国高等学校信息安全类专业在办学方面所迫切需要探讨的问题。教育部高等学校信息安全类专业教学指导委员会起草的《普通高等学校信息安全本科指导性专业规范》，按照“统一与特色相结合，宽口径，最小集合，最低标准，分类指导”的原则，对本专业的核心知识领域和知识单元的覆盖范围作了规定，旨在培养德、智、体等全面发展，掌握自然科学、人文科学基础和信息科学基础知识，系统掌握信息安全学的基本理论、技术和应用知识，并具备科学研究和实际工作能力的信息安全高级专门人才。

教育部为推进“质量工程”，自 2007 年 10 月开始，先后三批遴选了国家级特色专业建设点。目前，有十余所高校被批准为信息安全国家级特色专业建设点。在教材建设方面，2008 年 10 月，教育部高教司在《关于加强“质量工程”本科特色专业建设的指导性意见》中指出：“教材建设要反映教学内容改革的成果，积极推进教材、教学参考资料和教学课件三位一体的立体化教材建设，选用高质量教材，编写新教材。”为了适应新形势下对信息安全领域人才培养的需求，本届信息安全类专业教学指导委员会经过广泛深入调研，主要依托信息安全专业国家级特色专业建设点，与科学出版社共同组织出版本套《普通高等教育信息安全类国家级特色专业系列规划教材》，旨在贯彻专业规范和教学基本要求，总结和推广各特色专业建设点的教学经验和教学成果，提高我国信息安全专业本科教学的整体水平。

本套丛书在组织编写中，重点突出了以下几方面的特色。

1. 体现专业特色，贯彻专业规范和教学基本要求。依托“国家级特色专业建设点”，汇总优秀教学成果，将特色专业教育的内容、国内外科研教学的成果、信息安全专业规范与教学基本要求结合起来，内容安排围绕专业规范，体现核心知识单元与知识点。

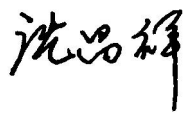
2. 按照分类指导原则，满足多层面的需求。针对同一类课程，根据不同的教学层次（普通院校、重点院校或研究型大学、应用型大学）和学时要求（多学时、少学时），涵盖不同范围的拓展知识单元，编写适合不同层面需求的教材。注重与先修课程、后续课程的有机衔接，每本书在重视系统性和完整性的基础上，尽量减少内容重复。

3. 拓宽专业基础，面向工程应用，加强实践环节。注重反映本学科领域的最新成果和发展方向，适当拓宽专业基础知识的范围，以增强所培养人才的适应性；面向工程应用，突出工科特色，反映新技术、新工艺；注重实践环节的设置，以促进学生的实际动手能力和创新能力的培养，真正使教材能够达到培养“厚基础、宽口径、会设计、可操作、能发展”人才的目的。

4. 注重立体化建设。本套丛书除了主教材外，还将逐步配套学习辅导书、教师参考书和多媒体课件等，为任课教师提供丰富的配套教学资源，方便教师教学，同时帮助学生复习与自学，使本套丛书更加易教易学。

本套丛书的编写汇聚了全国高校的优势资源，突出了多层次与适应性、综合性与多样性、前沿性与先进性、理论与实践的结合。在教材的组织和出版过程中得到了相关高校教务处及学院的帮助，在此表示衷心的感谢。

根据信息安全发展战略的要求，我们将对本套丛书不断更新，以保持教材的先进性和适用性。热忱欢迎全国同行以及关注信息安全领域教育及发展前景的广大有识之士对我们的工作提出宝贵意见和建议！



教育部高等学校信息安全类专业教学指导委员会主任委员

中国工程院院士

2011 年 4 月

前　言

随着计算机及计算机网络的发展，伴随而来的计算机病毒传播问题越来越引起人们的关注。尤其是近年来随着 Internet 的流行，有些计算机病毒借助网络爆发并传播，给广大计算机用户带来了极大的损失，同时也给网络应用安全带来严峻的挑战。面对这种新的形势和挑战，加强对新型计算机病毒的了解和认识就显得尤为重要。目前，“计算机病毒原理及技术”课程作为本科专业教学的一个重要部分，在很多高校都开设了这门课程。为了进一步加深该专业本科生，以及信息管理、计算机应用等相关专业学生对于计算机病毒知识的理解和掌握，提高学生对于计算机病毒的认识和应对能力，本书编者在广泛跟踪最新的计算机病毒技术和反病毒技术进展的基础上，充分吸收了相关技术发展的最新成果，使本书能紧跟业界最新技术的发展步伐和潮流。

本书有两个重要特点：一是在总结归纳计算机病毒工作机制等共性原理的基础上，着重对目前流行的各种典型计算机病毒的原理进行了仔细分析，内容由浅入深，循序渐进，能使读者在较短时间内掌握计算机病毒的基础知识，既能使初学者快速入门，又能使具有一定基础的读者得到进一步提高；二是结合丰富的实例，用通俗、简明的语言讲解了检测和防治各种计算机病毒的方法，一步步引导读者快速掌握反病毒技术的思路和技巧。同时，在每一章后面都附有相应的习题，以便读者对所学知识进一步理解和掌握。

本书共 10 章，主要内容包括计算机病毒概述、计算机病毒的工作机制、计算机病毒的表现、新型计算机病毒的发展趋势、计算机病毒检测技术、典型病毒的防范技术、网络安全、即时通信病毒和移动通信病毒分析、操作系统漏洞攻击和网络钓鱼概述、常用反病毒软件等。本书可作为高等学校信息安全本科专业基础课教材，也可作为信息管理和其他计算机应用专业的选修课教材，同时也适合广大计算机爱好者自学使用。阅读本书时，读者应具有计算机硬件、系统、网络方面的基础知识，并具有计算机方面的实际应用经验。

电子科技大学计算机学院秦志光教授担任本书主编并组织编写、修改、统稿和定稿，同时编写第 1 章，刘峤老师编写第 2～4 章和第 8 章，张凤荔老师编写第 5～6 章，刘彩霞、余圣协助张凤荔老师编写第 7 章、第 9 章和第 10 章。网络与数据安全四川省重点实验室团队的老师和博士生们在本书的编写过程中给予了无私帮助，编者在此致以深切谢意！

由于编者水平有限，书中难免存在不足和疏漏之处，请读者批评指正。编者很希望听到各位老师和读者们使用本书后的反馈意见，以利于我们今后进一步改进。

编　者

2012 年 4 月

目　录

第1章 计算机病毒概述

计算机病毒与医学上的“病毒”相比不完全相同，计算机病毒不是天然存在的，而是某些人利用计算机软、硬件所固有的弱点所编制的、具有特殊功能的程序。计算机病毒是一个程序，或一段可执行代码，它像生物病毒一样具有独特的复制能力，能够很快蔓延，有很强的感染性、一定的潜伏性、特定的触发性和极大的破坏性，又常常难以被根除。随着计算机网络的发展，计算机病毒与计算机网络技术结合，其蔓延的速度更加迅速。

计算机病毒是一个靠修改其他程序，并把自身复制品传染给其他程序的程序。计算机病毒是一种人为的计算机程序，这种程序隐藏在计算机系统的可存取信息资源中，利用计算机系统信息资源进行生存、繁殖，影响和破坏计算机系统的运行。在《中华人民共和国计算机信息系统安全保护条例》中对计算机病毒有明确的定义，病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”。

计算机的信息需要存取、复制和传送，计算机病毒作为信息的一种形式可以随之繁殖、感染和破坏，并且，当计算机病毒取得控制权之后，它会主动寻找感染目标、广泛传播。随着计算机技术发展得越来越快，计算机病毒技术与计算机反病毒技术的对抗也越来越激烈。从1983年计算机病毒被首次确认以来，直到1987年才开始在世界范围受到普遍的重视，至今全世界已经发现万余种病毒，并且还在快速增加。现在每天都要出现几十种新的计算机病毒，其中很多计算机病毒的破坏性非常大，稍有不慎，就会给计算机用户造成严重的后果。计算机操作系统的弱点往往被计算机病毒利用，所以一方面要提高系统的安全性以预防计算机病毒；另一方面，信息保密的要求又让人在泄密和截获计算机病毒之间无法选择。这样，计算机病毒与反计算机病毒势必成为一个长期的技术对抗过程。计算机病毒主要由反计算机病毒软件来对付，而且反计算机病毒技术将成为一项长期的科研任务。

1.1 计算机病毒的产生与发展

1.1.1 计算机病毒的起源

计算机病毒的来源多种多样，一般来自玩笑与恶作剧、报复心理、版权保护等方面，有的是计算机工作人员或业余爱好者纯粹为了寻求开心而制造出来的，有的则是软件公司为保护自己的产品不被非法复制而制造的报复性惩罚。还有一种情况就是蓄意破坏，它分为个人行为和政府行为两种：个人行为多为雇员对雇主的报复行为，而政府行为则是有组织的战略战术手段。对病毒的起源有几种说法。

第一种为科学幻想起源说。1977 年，美国科普作家托马斯·丁·雷恩推出轰动一时的《P-1 的青春》一书，作者构思了一种能够自我复制、利用信息通道传播的计算机程序，并称之为计算机病毒。这是世界上第一个幻想出来的计算机病毒。

第二种为恶作剧起源说。恶作剧者是为了显示一下自己在计算机技术方面的天赋，或是要报复一下他人或单位而编写的计算机病毒，只是和对方开个玩笑。而出发点有些恶意成分的人所编写的病毒的破坏性很大，世界上流行的许多计算机病毒都是恶作剧者的产物。

第三种是游戏程序起源说。20 世纪 70 年代，美国贝尔实验室的计算机程序员为了娱乐，在自己实验室的计算机上编制吃掉对方程序的程序，看谁能先把对方的程序吃光。有人猜测这是世界上第一个计算机病毒。

第四种是软件商保护软件起源说。软件制造商为了处罚那些非法复制者，在软件产品之中加入计算机病毒程序并由一定条件触发并传染。比如 Pakistani Brain 计算机病毒，该病毒是巴基斯坦的两兄弟为了追踪非法复制其软件的用户而编制的，它只是修改磁盘卷标，把卷标改为 Brain 以便识别。

归纳起来，计算机系统及 Internet 的脆弱性是产生计算机病毒的根本技术原因之一，人性心态与人的价值和法制的定位是产生计算机病毒的社会基础，基于政治、军事等方面的特殊目的是计算机病毒应用产生质变的催化剂。现在流行的病毒是人为故意编写的，从大量的统计分析来看，病毒作者主要情况和目的是一些天才的程序员为了表现自己和证明自己的能力，出于对上司的不满，为了好奇，为了报复，为了祝贺和求爱，为了得到控制口令，为了怕软件拿不到报酬而预留的陷阱等。当然也有因政治、军事、宗教、民族、专利等方面的需要而专门编写的病毒软件，其中也包括一些病毒研究机构和黑客的测试病毒软件。

1.1.2 计算机病毒的发展背景

1. 计算机病毒的祖先：Core War(磁芯大战)

早在 1949 年，距离第一部商用计算机的出现还有好几年时，计算机的先驱者冯·诺依曼就在他的一篇论文《复杂自动机组织论》中，提出了计算机程序能够在内存中自我复制的观点，即已把计算机病毒程序的雏形勾勒出来了。但在当时，绝大部分的计算机专家都无法想象这种会自我繁殖的程序是可能实现的，只有少数几个科学家默默地研究冯·诺依曼所提出的概念。直到 10 年之后，在美国电话电报公司(AT&T)的贝尔实验室中，3 个年轻程序员在工作之余想出一种电子游戏叫做 Core War(磁芯大战)，他们是道格拉斯·麦耀莱(H. Douglas McIlroy)、维特·维索斯基(Victor Vysottsky)及罗伯·莫里斯(Robert T. Morris)，当时 3 人的年纪都只有二十多岁。Core War 的玩法如下：双方各编写一套程序，输入同一部计算机中。这两套程序在计算机内存中运行，它们相互追杀。有时它们会放下一些关卡，有时会停下来修复被对方破坏的指令。当它们被困时，可以自己复制自己，逃离险境。因为它们都在计算机的内存(以前均用 Core 作为内存)中游走，因此叫 Core War。这个游戏的特点在于双方的程序进入计算机之后，玩游戏的人只能看着屏幕上显示的战况，而不能做任何更改，一直到某一方的程序被另一方的程序完全“吃掉”为止。

2. 计算机病毒的出现

在单机操作时代，每个计算机是互相独立的，如果有某部计算机因受到计算机病毒的感染

而失去控制，那么只需把它关掉即可。但是当计算机网络逐渐成为社会结构的一部分之后，一个会自我复制的计算机病毒程序很可能带来无穷的祸害。因此，长久以来，懂得玩“磁芯大战”游戏的计算机工作者都严守一条不成文的规则：不对大众公开这些程序的内容。

这项规则在1983年被打破了。科恩·汤普逊(Ken Thompson)是当年的一个杰出计算机得奖人。在颁奖典礼上，他做了一个演讲，不但公开地证实了计算机病毒的存在，而且还告诉所有听众怎样去写自己的计算机病毒程序。1984年，《科学美国人》*Scientific American* 月刊的专栏作家杜特尼(A. K. Dewdney)在5月写了第一篇讨论Core War的文章，并且只要寄上两美金，任何读者都可以收到他所写的有关编写这种程序的要领，并可以在自己家中的计算机上开辟战场。在1985年3月的《科学美国人》里，杜特尼再次讨论Core War和计算机病毒，在该文章中第一次提到“计算机病毒”这个名称。从此，计算机病毒就伴随着计算机的发展而发展起来了。

1.1.3 计算机病毒的发展历史

20世纪60年代初，美国电话电报公司(AT&T)的贝尔实验室Core War游戏问世。20世纪70年代早期的大型计算机时代，一些程序员制作了被称为“兔子”的程序，它们在系统中分裂出替身，占用系统资源，影响正常的工作。在一种大型计算机——Univax 1108系统中，首次出现了一个和现代计算机病毒本质上一样的叫做“流浪的野兽”(Pervading Animal)的程序，该程序可以将自己附着到其他程序的后面。20世纪80年代，独立程序员写了很多游戏或者其他的小程序，并通过电子公告板(BBS)自由地流传，窃取相关账号和密码，由此就诞生了无数的“特洛伊木马病毒”(Trojan Horses)。1982年，在苹果机上诞生了最早的引导区计算机病毒——“埃尔科克隆者”(Elk Cloner)。

到1986年，随着计算机病毒数量的不断增大，计算机病毒的制作技术也逐步提高。计算机病毒是所有软件中最先利用操作系统底层功能，以及最先采用复杂的加密和反跟踪技术的软件之一，计算机病毒技术发展的历史就是软件技术发展的历史。一种新的病毒技术出现后，计算机病毒会迅速发展；接着，反计算机病毒技术的发展又会抑制其流传。操作系统进行升级时，计算机病毒也会调整为新的方式，产生新的计算机病毒技术。

计算机病毒的发展历程可以分为以下4个阶段。

第一代病毒(1986～1989年)，这期间出现的病毒称之为传统的病毒，为萌芽与滋生时期。

第二代病毒(1989～1991年)为混合型病毒，是病毒由简单到复杂、由单纯到成熟的阶段。

第三代病毒(1992～1995年)为多态性病毒、自我变形病毒，为病毒成熟发展阶段。

第四代病毒(1996～今)，随着Internet的普及，病毒的流行迅速突破地域的限制而传播。

1. *第一代病毒——病毒的萌芽时期*

第一代病毒产生于1986～1989年，称为传统的病毒，是计算机病毒的萌芽和滋生时期。由于那时计算机的应用软件少，且大多是单机运行环境，病毒的种类有限，病毒的清除工作相对来说较容易。这一阶段的计算机病毒具有如下的一些特点。

(1)病毒攻击的目标比较单一，传染磁盘引导扇区，或传染可执行文件。

(2)病毒程序主要采取截获系统中断向量的方式监视系统的运行状态，并在一定的条件下对目标进行传染。

(3)病毒传染目标以后的特征比较明显,如磁盘上出现坏扇区、可执行文件的长度增加、文件建立日期时间发生变化等。

(4)病毒程序不具有自我保护的措施。

随着计算机反病毒技术的提高和反病毒产品的不断涌现,病毒编制者也在不断地总结自己的编程技巧和经验,千方百计地逃避反病毒产品的分析、检测和解毒,从而出现了第二代计算机病毒。

2. 第二代病毒——混合型病毒

第二代病毒称为混合型病毒(或"超级病毒"),年限为 1989～1991 年,它是计算机病毒由简单发展到复杂、由单纯走向成熟的阶段。当时计算机局域网开始应用与普及,应用软件开始转向网络环境,网络系统尚未有安全防护的意识,缺乏在网络环境下防御病毒的思想准备与方法对策,使计算机病毒形成了第一次流行高峰。这一阶段的计算机病毒具有如下特点。

(1)病毒攻击的目标趋于混合型,可以感染多个/种目标。

(2)病毒程序采取隐蔽的方法驻留内存和传染目标。

(3)病毒传染目标后没有明显的特征。

(4)病毒程序采取了自我保护措施,如加密技术、反跟踪技术,制造障碍,增加人们剖析和检测病毒、解毒的难度。

(5)出现许多病毒的变种,这些变种病毒较原病毒的传染性更隐蔽,破坏性更大。

这一时期出现的病毒不仅在数量上急剧增加,更重要的是病毒从编制的方式、方法,驻留内存以及对宿主程序的传染方式、方法等方面都有了较大的变化。

3. 第三代病毒——多态性病毒

第三代病毒的产生年限为 1992～1995 年,此类病毒称为"多态性"病毒或"自我变形"病毒。所谓"多态性"或"自我变形",是指此类病毒在每次传染目标时,放入宿主程序中的病毒程序大部分都是可变的,即同一种病毒的多个样本中,病毒程序的代码绝大多数是不同的。

此类病毒的首创者是 Mark Washburn,他是一位反病毒的技术专家,他编写的"1260 病毒"就是一种多态性病毒,该病毒有极强的传染力,被传染的文件被加密,每次传染时都更换加密密钥,而且病毒程序都进行了相当大的改动。他编写此类病毒的目的是为了研究,以证明特征代码检测法不是在任何场合下都是有效的。不幸的是,为研究病毒而发明的此种病毒超出了反病毒的技术范围,流入了病毒技术中。

1992 年上半年,在保加利亚发现了"黑夜复仇者"(Dark Avenger)病毒的变种 MutationDark Avenger,这是世界上最早发现的多态性的实战病毒,它可用独特的加密算法产生几乎无限数量的不同形态的同一病毒。据悉,该病毒作者还散布一种名为"多态性生成器"的软件工具,利用此工具将普通病毒进行编译即可使之变为多态性病毒。

1992 年早期,第一个多态性计算机病毒生成器 MtE 被开发出来,计算机病毒爱好者利用这个生成器生成了很多新的多态计算机病毒。同时,第一个计算机病毒构造工具集(Virus Construction Sets)——"计算机病毒创建库"(Virus Create Library)开发成功,这类工具的典型代表是"计算机病毒制造机"(VCL),它可以在瞬间制造出成千上万种不同的计算机病毒,查解时不能使用传统的特征识别法,需要在宏观上分析指令,解码后才能查解计算机病毒。变体机就是增加解码复杂程度的指令生成机制。这段时期出现了很多非常复杂的计算机病毒,