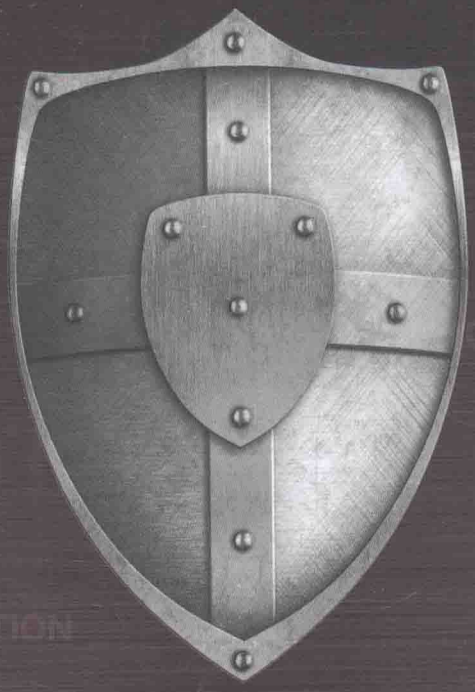
“十二五”普通高等教育本科国家级规划教材
21世纪高等教育信息安全系列规划教材



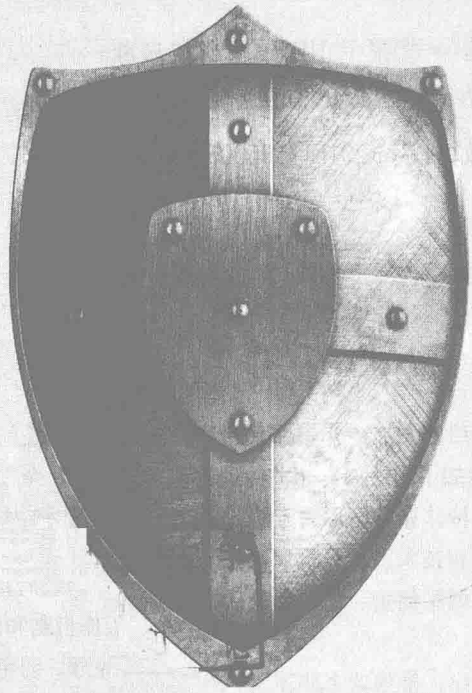
计算机病毒原理与防范

（第2版）

秦志光 张凤荔◎主编

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

“十二五”普通高等教育本科国家级规划教材
21世纪高等教育信息安全系列规划教材



计算机病毒原理与防范

（第2版）

秦志光 张凤荔◎主编

人民邮电出版社
北京

图书在版编目（CIP）数据

计算机病毒原理与防范 / 秦志光，张凤荔主编. -- 2版. -- 北京 : 人民邮电出版社，2016.1
21世纪高等教育信息安全系列规划教材
ISBN 978-7-115-37567-4

Ⅰ. ①计… Ⅱ. ①秦… ②张… 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(2015)第056054号

内 容 提 要

随着计算机及计算机网络的发展，伴随而来的计算机病毒的传播问题越来越引起人们的关注。本书在第 1 版的基础上，增加了网络病毒相关的理论和技术内容，全面介绍了计算机病毒的工作机制与原理以及检测和防治各种计算机病毒的方法。主要内容包括计算机病毒的工作机制和发作表现，新型计算机病毒的主要特点和技术，计算机病毒检测技术，典型计算机病毒的原理、防范和清除，网络安全，系统漏洞攻击和网络钓鱼、即时通信病毒和移动通信病毒分析、常用反病毒软件的使用技巧，以及 6 个综合实验。

本书内容全面，深入浅出，能使读者快速掌握计算机病毒的基础知识及反病毒技术的思路和技巧。本书可以作为高等学校信息安全本科专业基础教材，也适合信息管理和其他计算机应用专业作为选修课教材，同时也适合广大计算机爱好者自学使用。

◆ 主　　编　秦志光　张凤荔
责任编辑　邹文波
责任印制　沈　蓉　彭志环
◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京昌平百善印刷厂印刷
◆ 开本：787×1092　1/16
印张：22.25　　2016 年 1 月第 2 版
字数：532 千字　　2016 年 1 月北京第 1 次印刷

定价：49.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

21世纪高等教育信息安全系列规划教材

编 委 会

第 2 版前言

计算机的出现给人们的生活带来了前所未有的便利，然而人们在享受科技进步的同时，也经常遭受计算机病毒的困扰。计算机病毒是一种人为的程序代码，是信息社会发展到一定程度的产物，是犯罪领域的一种新方式。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了。为了进一步加深信息安全专业本科生以及信息管理、计算机应用等相关专业学生对计算机病毒知识的理解和掌握，提高学生对计算机病毒的认识和应对能力。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，充分吸收相关技术发展的最新成果，结合教学编写了本书。

本书自出版以来，多次印刷，得到了广大高校师生的认可。2012 年，本书被评为国家“十二五”规划教材。本次改版，编者在第 1 版的基础上，结合近几年教学改革实践及反病毒技术的发展，对全书内容进行了优化、补充和完善，使本书更适合人才培养的需要。

本书第 2 版的内容修订如下：

1．在第 1 章中增加了网络病毒、系统漏洞、即时通信病毒、手机病毒的特点分析；

2．将第 1 版的第 2 章传统计算机病毒的工作机制与第 3 章计算机病毒的表现合并为一章，即第 2 版的第 2 章传统计算机病毒的工作机制及发作表现；

3．在第 3 章新型计算机病毒的发展趋势及特点和技术中，针对最近流行病毒的特点与发展趋势进行了分析与说明；

4．在第 4 章计算机病毒检测技术中增加了网络病毒的检测技术；

5．在第 5 章典型计算机病毒的原理、防范和清除中增加了典型蠕虫、后门、黑客等病毒的分析、清除和防范技术；

6．在第 6 章网络安全中，对最近网络安全的相关事件进行了分析和说明；

7．增加了第 7 章系统漏洞攻击和网络钓鱼概述以及第 8 章即时通信病毒和移动通信病毒分析的内容；

8．在第 9 章常用反病毒软件中的软件产品介绍中，去掉了一些过时的产品，增加了一些最新流行产品的功能分析和介绍；

9．增加了一个附录，设计了 6 个综合实验，给出了实验的原理和具体实现步骤等内容。

本书的重要特点体现在两个方面：一是本书编者在总结归纳出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性的计算机病毒的原理进行了仔细的分析，内容从浅到深，循序渐进，深入浅出，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的提高；二是结合丰富的实例，用通俗、简明的语言图文并茂地讲解了检测和防治各种计算机病毒的方法，步步引导读者快速掌握反病毒技术的思路和技巧。同时，每一章后面都附有相应的练习题帮助读者对本章所

学知识进一步理解和掌握。

本书可以作为高等学校信息安全本科专业基础教材，也适合信息管理和其他计算机应用专业作为选修课教材，同时也适合广大计算机爱好者自学使用。阅读本书时，读者应了解计算机的硬件、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。本书作为教材使用时，建议学时为60学时，各章学时分配如下：

章	学时数	章	学时数
第1章	4	第6章	8
第2章	8	第7章	6
第3章	4	第8章	6
第4章	8	第9章	2
第5章	14		

本书由电子科技大学计算机学院秦志光和张凤荔担任主编并组织编写、修改、统稿和定稿，非常感谢在使用第1版图书过程中提出改进意见的各位老师，根据这些意见本书增加了一些编程作业和实验的内容，希望能够锻炼学生的动手能力。感谢电子科技大学软件学院刘峤老师完成了第8章内容的写作；感谢计算机学院的秦科老师，他使用本书的内容进行了教学活动，并提出了一些教学的建议和实验的内容；感谢电子科技大学计算机学院的韩宏老师，他指导学生设计和实现实验的内容，并对实验的过程和程序进行了详细的分析、设计和实现；感谢刘宇江、陈培俊同学实现了实验的编码并调试完成；感谢电子科技大学四川省网络与数据安全重点实验室的老师和博士生们在本书的编著过程中给予的无私帮助！

由于编者水平有限，书中难免存在错误之处，请读者批评指正。编者很愿意听到各位老师和同学们在使用本教材时的反馈意见，读者的反馈意见将有利于我们今后进一步改进。

编　者

2015年3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”不同，它不是天然存在的，而是某些人利用计算机软、硬件所固有的脆弱性，编制的具有特殊功能的程序。由于它与生物医学上的“病毒”同样有传染和破坏的特性，例如，具有自我复制能力、很强的感染性、一定的潜伏性、特定的触发性和很大的破坏性等，因此由生物医学上的“病毒”概念引申出“计算机病毒”这一名词。

从广义上定义，凡是能够引起计算机故障、破坏计算机数据的程序统称为计算机病毒。依据此定义，诸如“逻辑炸弹”、“蠕虫”等均可称为计算机病毒。在国内，专家和研究者对计算机病毒也做过不尽相同的定义，但一直没有公认的明确定义，直至 1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在条例第二十八条中明确指出：“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者毁坏数据，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。”此定义具有法律性、权威性。

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，它们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尖锐。据统计，现在基本上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都非常大，计算机用户稍有不慎，就会给病毒可乘之机，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，提高系统的安全性是预防计算机病毒的一个重要方面，但完美的系统是不存在的，提高一定的安全性必然会使系统让更多时间用于计算机病毒检查，系统也就失去了部分可用性与实用性；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形成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，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。另外，有的计算机病毒还是为研究或实验而设

计的“有用”程序，由于某种原因失去控制扩散出去，从而成为危害四方的计算机病毒。计算机病毒的起源到现在还没有一个确切的说法，下面是其中有代表性的几种。

1. 科学幻想起源说

1977年，美国科普作家托马斯·丁·雷恩推出了轰动一时的《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。人类社会有许多现行的科学技术，都是在先有幻想之后才成为现实的。因此，不能否认这本书的问世对计算机病毒的产生所起的催化作用。

2. 恶作剧起源说

恶作剧者大多是那些对计算机知识和技术均有兴趣的人，并且特别热衷那些别人认为是不可能做成的事情，因为他们认为世上没有做不成的事。这些人或是要显示一下自己在计算机知识方面的天赋，或是要报复一下他人或单位。这其中前者是无恶意的，所编写的计算机病毒也大多不是恶意的，只是和对方开个玩笑，显示一下自己的才能以达到炫耀的目的。后者的出发点则多少有些恶意成分在内，所编写的病毒往往比前者的破坏性要大一些，世界上流行的许多计算机病毒是恶作剧者的产物。

3. 游戏程序起源说

20世纪70年代，计算机在社会上还没有得到广泛的普及应用，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。

4. 软件商保护软件起源说

计算机软件是一种知识密集型的高科技产品，由于对软件资源的保护不尽合理，使得许多合法的软件被非法复制，从而使得软件制造商的利益受到了严重的侵害，因此，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。例如，Pakistani Brain 计算机病毒在一定程度上就证实了这种说法，该计算机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。也正因为如此，当计算机病毒出现之后，有人认为这是由软件制造商为了保护自己的软件不被非法复制所致。

关于计算机病毒起源的原因还有一些其他说法。归纳起来，计算机系统、Internet 的脆弱性是产生计算机病毒的根本技术原因之一，计算机科学技术的不断进步和快速普及应用是产生计算机病毒的加速器。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。

1.1.2 计算机病毒发展背景

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，即已把计算机病毒程序的蓝图勾勒出来，但当时，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）、