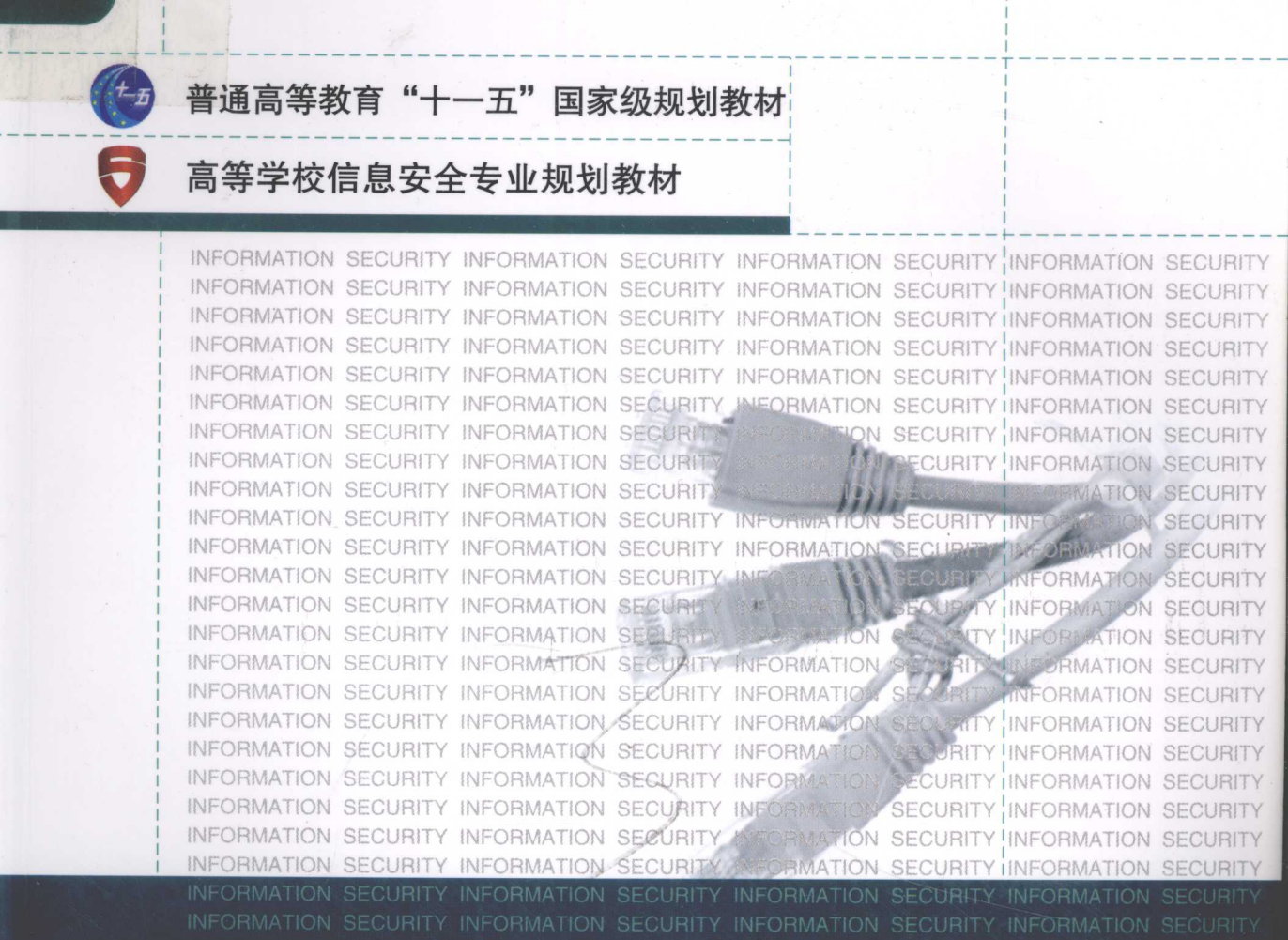
普通高等教育“十一五”国家级规划教材

高等学校信息安全专业规划教材



计算机病毒分析与对抗

第二版

傅建明 彭国军 张焕国 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

普通高等教育“十一五”国家级规划教材

高等学校信息安全专业规划教材

计算机病毒分析与对抗

第二版

傅建明 彭国军 张焕国 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

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.—2版.—武汉:武汉大学出版社,2009.11

普通高等教育"十一五"国家级规划教材

高等学校信息安全专业规划教材

ISBN 978-7-307-07400-2

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

中国版本图书馆CIP数据核字(2009)第192718号

责任编辑:林 莉 责任校对:刘 欣 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:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:湖北睿智印务有限公司

开本:787×1092 1/16 印张:21.25 字数:536千字 插页:1

版次:2004年4月第1版 2009年11月第2版

2009年11月第2版第1次印刷

ISBN 978-7-307-07400-2/TP·344 定价:35.00元

高等学校信息安全专业规划教材

编　委　会

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护技术。特别是在计算机病毒的产生机理、感染特点、传播方式、危害表现以及防护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。全书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，此外还对木马和 Rootkit 等破坏性程序的功能和原理进行了分析。在病毒防护方面，本书重点阐述了常见的病毒检测对抗技术，分析了用户在进行日常操作过程中遇到的各类安全问题，并给出了具体的防护思路和手段。

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，也可用做计算机安全职业培训的教材。

序 言

二十一世纪是信息的时代，信息成为一种重要的战略资源。信息科学成为最活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业成为世界第一大产业。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，必须采取措施确保我国的信息安全。

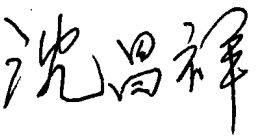
发展信息安全技术与产业，人才是关键。培养信息安全领域的专业人才，成为当务之急。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准武汉大学建立信息安全博士点。现在，全国设立信息安全本科专业的高等院校已增加到 70 多所，设立信息安全博士点的高等院校和科研院所也增加了很多。2007 年“教育部高等学校信息安全类专业教学指导委员会”正式成立，并在武汉大学成功地召开了“第一届中国信息安全学科建设与人才培养研讨会”。我国信息安全学科建设与人才培养进入蓬勃发展阶段。

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，2003 年武汉大学组织编写了一套《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。这套丛书出版后得到了广泛的应用，深受广大读者的厚爱，为传播信息安全知识发挥了重要作用。现在，为了能够反映信息安全技术的新进展、更加适合信息安全教学的使用和符合信息安全类专业指导性专业规范的要求，武汉大学对原有丛书进行了升版。

我觉得升版后的这套新教材的特点是内容全面、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，符合信息安全类专业指导性专业规范的要求，适合教学使用。在我国信息安全专业人才培养蓬勃发展的今天，这套新教材的出版是非常及时的和十分有益的。

我代表编委会对图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，以便能够进一步修改完善。

中国工程院院士，武汉大学兼职教授



2008 年 8 月 28 日

前 言

随着计算机和互联网技术的快速发展与广泛应用，计算机及网络系统的安全受到严重挑战，来自计算机病毒和黑客攻击等方面的威胁越来越大。近年来，恶意软件数量急剧增加，各类病毒免杀技术不断推陈出新，传统的反病毒技术和手段受到了极其严重的挑战。与此同时，病毒产业链日趋成熟，恶意软件的经济目的性越来越强，在不断融合各类技术以及社会工程手段滞后的情况下，恶意软件令人防不胜防。

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 CIH、爱虫、Slammer、冲击波、震荡波、扫荡波、极速波、网银大盗、熊猫烧香、磁碟机、机器狗等无不给广大用户带来了巨大的损失。了解计算机病毒的原理、掌握计算机病毒的防护技术，将有利于有效地对抗计算机病毒。

本书第 1 章从生物病毒的概念入手，介绍了计算机病毒的起源、产生、定义、特征、分类，以及发展等，并对计算机病毒及其对抗技术进行了分析。这些内容构成了本书的第 1 章。通过本章的学习，读者能较全面地了解计算机病毒等破坏性程序的基本概念和基本的防护知识。

计算机病毒涉及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 2 章从一个简单的计算机病毒伪代码出发，引入计算机病毒的逻辑结构，进而介绍了计算机的磁盘管理、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。该章能为读者提供计算机病毒的基本系统知识。

第 3 章重点阐述了计算机病毒的传播、触发以及破坏机制。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的。

第 4 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 5 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、脚本病毒和恶意网页的原理和特征，并对相关病毒的源码进行了分析。这两章从感性上介绍病毒，从原理上分析病毒，从而有利于剖析病毒的本质。

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，第 6 章分析了目前计算机病毒经常采用的各种抗分析技术，包括自我隐藏技术、花指令、简单自加密、多态、变形、加壳、代码优化、脚本加密及异常处理技术等。这些技术的综合运用给病毒的检测带来较大困难。

目前 ODay 漏洞频发，这给计算机和网络安全带来了重大安全隐患。第 7 章介绍了漏洞机理以及网络蠕虫的传播原理，并给出了实例分析。第 8 章对目前流行的木马功能、原理及流行的 Rootkit 技术进行了分析，并给出了实例分析。

第 9 章主要介绍了目前流行的各类反病毒技术和手段。本章对特征值检测技术、校验和

检测技术、行为监测技术、启发式扫描技术、虚拟机技术及主动防御技术进行了介绍，接着介绍了病毒的清除方法和手段。

第 10 章针对恶意软件的传播周期和渠道，给出了个人用户在使用个人电脑时针对恶意软件攻击的一些安全防护策略、手段和技术。

除了 DOS 和 Windows 平台下的病毒外，还有许多其他操作系统的病毒，如 UNIX、LINUX、OS/2、MAC 下的病毒。第 11 章首先概述了其他平台的病毒，重点介绍 UNIX/LINUX 下 ELF 的文件格式、基于 ELF 的计算机病毒原理，以及 OS/2 和 Mac OS 下的计算机病毒，最后本章还对手机病毒进行了介绍。

本书是在 2004 年武汉大学出版社出版的《计算机病毒分析与对抗》一书的基础上改版而成的。

由于计算机病毒与反病毒技术发展迅猛，计算机病毒的定义及其传播方式已经发生了很大改变，反病毒技术相应也出现了较大变化。

在教学和本次改版过程中，我们发现，原有的一些关于计算机病毒的论述已经不够准确，甚至有些观点在目前看来已经过时。因此，本书基于目前流行的病毒技术与反病毒技术现状，对原书做了较大篇幅改写和整理。为了使本书内容与时俱进，我们增加了部分章节（第 7、8、10 章）；同时为了缩减本书篇幅，我们对原书各章内容都进行了精简并删除了之前的若干章节（如原书第 9 章：计算机病毒的理论模型，以及第 11 章：计算机病毒样本的提取）。改版之后的本书更能够体现目前最新的病毒与反病毒发展技术和趋势。

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。在本书的改版过程中，程斌林、乔伟、刘新文、熊思阳、张志峰、徐颖、许静和朱禅元等同学做了一定的文字整理工作，在此向他们表示感谢。

由于时间和水平有限，难免有错，恳请读者批评指正，以使本书得以改进和完善。

作　者

2009 年 9 月于珞珈山

目 录

第1章 计算机病毒概述

在自然界里，存在各式各样的病毒影响着各类生物，它们或潜伏在生物体内并不具有破坏性，或者大规模爆发导致严重的社会问题。近年来的甲型 H1N1、SARS、禽流感、AIDS 等都是由病毒感染引发的。在计算机网络世界里，同样也存在着会对计算机系统带来危害的计算机病毒，它们对社会造成的负面影响和损失也是令人刻骨铭心的，2003 年的“冲击波”、2006 年的“熊猫烧香”、2008 年的“机器狗”曾给广大用户带来了巨大的损失。

随着互联网的飞速发展，计算机病毒技术也在不断迅速发展，病毒数量和类型都在不断增多。计算机病毒的定义也不再如过去一般狭隘，现在的病毒结合各类技术来入侵计算机，常见的病毒种类很多，如蠕虫、木马、后门、恶意脚本、Rootkit、流氓软件、间谍软件、广告软件、Exploit、黑客工具等，其定义越来越泛化模糊，可以简单地说，凡是带有恶意目的的程序或代码都是计算机病毒。

了解计算机病毒的原理、基本防御以及对抗措施，有利于正确认识计算机病毒和有效地对抗计算机病毒以减少计算机病毒造成的损失。本章从生物病毒出发，分析计算机病毒与生物病毒的联系和区别，介绍计算机病毒的分类、来源及其发展。

1.1 生物病毒

1.1.1 生物病毒的概述

在生物界，病毒是目前发现的最小微生物，且只能存在于活的生物体中。虽然它们是如此的微小，但一旦进入宿主的细胞，就会给宿主造成极大的伤害。不管是动物还是植物都难逃病毒的攻击，比如说一般的感冒、疱疹和肝炎都是病毒所引成的疾病。在过去二十年，最严重的疾病——AIDS（acquired immunity deficiency syndrome）是由“HIV”(human immunodeficiency virus)病毒所引起的。特别是，2003 年的严重呼吸综合征 SARS（severe acute respiratory syndrome）是由冠状病毒造成的疾病，2009 年的甲型 H1N1 流感是 Orthomyxoviridae 系列病毒造成的疾病，它们传染性极强。

病毒(virus)是一类比细菌还小的非细胞形态的生物。它们与其他生物相比显然不同，其突出的特点是：

（1）个体极小。大多数病毒都比细菌小得多，须借助电子显微镜才能看见。细菌的大小一般以微米表示，而病毒的大小则以纳米表示。

（2）寄生性。病毒没有独立的代谢活动，它们只能在特定的、活的宿主细胞中繁殖，脱离宿主细胞便不能进行任何形式的代谢，在活体外不具有任何生命特征。

（3）没有细胞结构，化学组成与繁殖方式较简单。病毒没有细胞结构，大多数病毒是由蛋白质与核酸组成的大分子，而且只含单一类型核酸 DNA 或 RNA。目前尚未发现含两类核

酸的病毒。病毒的繁殖方式不是通过二分分裂，因为病毒不具备其繁殖所需的组织，它必须依赖于宿主细胞进行复制。

可以认为，病毒是超显微的、没有细胞结构的、专寄生于活细胞的大分子微生物，它们在活体外具有一般大分子特征，一旦进入宿主细胞又呈现生命特征。

1.1.2 生物病毒的结构

电子显微镜及X射线衍射技术的发展，有可能观察并分析病毒的空间细微结构。研究病毒结构，对了解它们的功能与进化、认识病毒的本质以及对病毒的分类鉴定都有重要意义。

现已观察到很多病毒均具有共同的结构形式。病毒的最小形态单位为衣壳粒（capsomere）。衣壳粒是由一种或几种多肽链折叠而成的蛋白质亚单位。衣壳粒以对称形式有规律地排列，构成病毒的蛋白质外壳，称为衣壳（capsid）。衣壳的中心包含着病毒的核酸即核髓。衣壳与病毒核髓合称核衣壳（nucleocapsid）。有些病毒核衣壳是裸露的，有些病毒在核衣壳外还由被膜（envelope）包围着。完整的、具有感染性的病毒颗粒称为病毒粒子（virion）。无被膜的病毒粒子由核衣壳组成，有被膜的病毒粒子则由被膜与核衣壳组成。这样的结构具有高度的稳定性，保护病毒核酸不致在细胞外环境中受到破坏。

1.1.3 生物病毒的繁殖

病毒是专性细胞内寄生物，它们只能在活细胞内繁殖，而不能在一般培养基中繁殖。现在培养病毒除用敏感动物（如小白鼠、豚鼠、家兔、猴等）、鸡胚培养外，还发展到用活的组织或细胞培养。病毒从其宿主中分离出来后，可以使它们在合适的组织细胞中增殖，噬菌体则在其宿主细胞中繁殖，并得到大量病毒子孙。病毒在活细胞中的繁殖方式不是二分分裂，而是感染细胞后，“接管”宿主细胞的生物合成机构，使之按照病毒的遗传特性，合成病毒的核酸与蛋白质，然后聚集成新的病毒粒子。这种繁殖方式与一般生物的繁殖方式根本不同，称为病毒的复制。无论是动物病毒、植物病毒或细菌病毒，其繁殖过程虽不完全相同，但基本相似。研究得比较多的是大肠杆菌T系噬菌体。病毒感染宿主细胞进行繁殖的过程可分为吸附、侵入、复制和聚集等。

1. 吸附

吸附是病毒感染细胞的第一步。病毒对宿主细胞的吸附有高度特异性。如噬菌体并非吸附在细菌细胞表面的任何一点，而是吸附在细菌表面某特定的受体上。受体实际上是细胞表面的一定化学组成部分。曾经从大肠杆菌抽提得到与大肠杆菌噬菌体T5吸附有关的受体。经过抽提的细菌不能再被噬菌体T5吸附，但仍被T2、T4与T6噬菌体吸附。经该抽提处理后的T5，不能再吸附于正常宿主细胞上。

吸附是噬菌体感染细菌的必经阶段。当敏感细菌发生突变，而不再被某一噬菌体吸附时，便成为抗该噬菌体的抗性菌株。同样，病毒也可发生突变而又成为可吸附的。

2. 侵入

病毒侵入的方式决定于宿主细胞的性质。具有细胞壁的细胞（如细菌）与没有细胞壁的细胞（如动物细胞）的侵入方式不一样。最复杂的侵入方式见于噬菌体对细菌的感染。大肠杆菌噬菌体T4借其尾部末端附着到敏感细菌表面，并借其尾丝帮助固定在细胞上。尾部的酶水解细胞壁肽聚糖，使细胞壁产生一个小孔，然后尾鞘收缩，将尾髓压入细胞。尾髓为一空管，通过尾髓，噬菌体头部的DNA被注入细菌细胞，蛋白质外壳则仍留在细胞外。