Leader 灵创

灵创职业教育 • 网络与信息安全系列教材

计算机病毒防护

李 剑 刘正宏 沈俊辉 主编

北京邮电大学出版社
www.buptpress.com

灵创职业教育·网络与信息安全系列教材

计算机病毒防护

李　剑　刘正宏　沈俊辉　主编

北京邮电大学出版社
·北京·

内 容 简 介

作为一本信息安全教材，本书介绍了计算机病毒原理与防治。书中内容共9章，第1章是计算机病毒概述；第2章是计算机病毒的工作机制；第3章是计算机病毒的表现；第4章是计算机病毒的发展趋势及特点和技术；第5章是计算机病毒检测技术；第6章是典型计算机病毒的原理、防范和清除；第7章是防范恶意代码技术；第8章是常用防病毒软件；第9章是中国计算机病毒法律与制度建设。除了以上内容之外，书中还介绍了大量的实验、实践、例子等内容。

本书适合于高等职业技术学校或高等专科学校信息安全相关专业的学生进行计算机病毒原理与防治方面的教育。

图书在版编目(CIP)数据

计算机病毒防护/李剑，刘正宏，沈俊辉主编. —北京：北京邮电大学出版社，2009

ISBN 978-7-5635-1912-5

Ⅰ.计… Ⅱ.①李…②刘…③沈… Ⅲ.计算机病毒—防治—教材 Ⅳ.TP309.5

中国版本图书馆CIP数据核字(2009)第058798号

书　　名：计算机病毒防护
作　　者：李　剑　刘正宏　沈俊辉
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)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京市梦宇印务有限公司印刷
开　　本：787 mm×1 092 mm　1/16
印　　张：9.25
字　　数：228千字
印　　数：1—3 000册
版　　次：2009年6月第1版　2009年6月第1次印刷

ISBN 978-7-5635-1912-5　　定　价：16.00元

灵创职业教育·网络与信息安全系列教材

编 委 会

序

目前我国“职业教育”正值春天。在党和国家的大力支持和积极推动下，全社会对职业教育的关注空前高涨，职业教育蓬勃发展。值此大好时机，每个教育工作者都应认真贯彻落实科学的发展观，坚持以服务为宗旨，以就业为导向，以提高质量为重点，进一步解放思想、开拓进取、扎实有力地推进我国职业教育又好又快地发展，办好人民满意的职业教育。但出于历史原因，目前我国职业教育体系很不健全，职教专业、职教教材“本科简化型”现象比较普遍，真正“重实践，重应用，与职业技能培养紧密结合”的高质量精品教材非常紧缺。

鉴于上述情况，为促进我国职业教育的规范发展，特别是为了满足当前各级各类职业教育教师、学生对适配自身教育和实践教材的迫切需要，北京邮电大学出版社，灵创团队北京邮电大学信息安全中心，灵创团队北京邮电大学数字内容研究中心以及绵阳灵创电子信息技术学校的专家、领导，决定共同合作，团结全国相关领域专家，策划、撰写、出版多套覆盖“网络与信息安全”和“数字媒体创意”等领域的“灵创职业教育”系列教材。

在“灵创职业教育·网络与信息安全”系列教材策划过程中，我们组织安全和职教专家对国内目前“网络与信息安全”职教层次人才需求和“网络与信息安全”职教发展现状进行了全面调研分析。研究发现，社会对“网络与信息安全”职教层次的人才需求集中在“信息与网络安全管理”、“安全产品营销与服务”方面。下表显示了对这些岗位职业技能需求和学习领域进行研究分析的结果。

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	管理、维护操作系统，保障操作系统级安全	1. 系统及应用安全风险评估 2. 系统及应用安全方案设计 3. 系统安全配置 4. 系统安全监控及审计 5. 数据安全 6. 应用系统运行安全	1. 信息安全法规/标准 2. 操作系统访问控制配置 3. 操作系统进程及服务配置 4. 操作系统性能、本地/网络访问监控 5. 系统日志管理 6. 数据备份恢复 7. 漏洞管理 8. 操作系统安全风险分析及工具	1. 信息安全法规与标准 2. 操作系统管理 3. 信息安全导论(操作系统安全部分) 4. 信息安全管理与工程(信息安全风险评估-操作系统)

续表

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	管理、维护数据库，保障数据库系统安全运行及数据安全	1. 数据库安全风险评估 2. 数据库安全管理方案设计 3. 数据库安全管理	1. 数据库基本概念 2. 数据库基本管理操作 3. 数据安全管理操作（包括数据库访问控制安全、数据库备份恢复） 4. 数据库安全风险分析及工具	1. 信息安全导论（数据库安全部分） 2. 信息安全管理与工程（信息安全风险评估-数据库）
	管理、维护信息服务，保障信息服务安全运行	1. 安装、配置常见的网络服务 2. 制作网站	1. 常见网络服务器安装、配置、管理 2. 网站制作 3. 网络服务安全	1. 网站制作 2. 网络服务管理与维护 3. 信息安全导论（网络服务安全）
	病毒防护	1. 设计系统计算机病毒防范方案 2. 防毒软件采购 3. 安装和配置计算机病毒软件 4. 防毒软件维护	1. 操作系统原理 2. 计算机病毒原理 3. 防毒软件产品 4. 防毒软件安装、配置、升级管理	1. 计算机病毒防范 2. 信息安全产品与方案
	管理、维护网络，保障网络安全	1. 构建基础网络连接 2. 网络安全风险分析 3. 网络安全方案设计 4. 网络安全设备配置 5. 网络安全监控	1. 网络基础，包括局域网构建、网络协议、常见网络设备交换机、路由器配置管理 2. 网络安全与管理，包括防火墙、VPN、IDS 技术及配置管理基本操作，网络攻击与防护简介 3. 网络攻击与防范，包括各类网络攻击原理，防范手段（如入侵检测、防火墙、VPN 等防范手段的使用）	1. 网络安全与管理 2. 网络攻击与防范技术 3. 信息安全管理与工程（信息安全风险评估－网络安全） *4. 入侵检测技术 *5. 防火墙技术 *6. 黑客防范
	保障物理和环境安全	1. 提出信息系统场地安全需求及建设方案，监控、审计场地安全方案实施情况 2. 提出信息系统自然防灾需求及建设方案，监控和审计防灾方案实施情况 3. 规划设计信息系统物理访问控制方案，监控和审计方案实施情况	1. 电路电工基础 2. 信息系统场地安全、防灾等相关法规、标准 3. 信息系统物理访问控制相关产品	1. 信息安全导论（信息系统物理与环境安全） 2. 信息安全管理与工程 3. 信息安全产品与方案
	信息保密管理	1. 制定信息系统信息保密与数字权益保护方案 2. 采购信息保密、数字权益保护产品 3. 信息保密、数字权益保护方案实施	1. 密码学基础 *2. 信息隐藏、数字水印、数字权益保护	1. 信息安全导论 2. 信息安全产品与方案（信息隐藏） 3. 信息安全管理与工程（信息保密）
	信息安全工程管理	1. 设计信息安全体系 2. 采购信息安全产品 3. 管理控制信息安全工程 4. 制定信息安全管理方案	1. 信息安全体系架构 2. 信息安全法规、标准 3. 信息安全管理方案文档编制	1. 信息安全导论 2. 信息安全管理与工程

续表

职业目标	岗位主要职责	职业技能要求	学习领域	
			知识	整合课程
信息与网络安全管理	信息安全策略、信息安全制度制定	1. 分析企业信息系统安全风险 2. 制定全面的安全管理策略和制度	1. 信息安全体系架构 2. 信息安全法规、标准 3. 信息安全管理方案文档编制	1. 信息安全导论（信息安全体系） 2. 信息安全管理与工程（安全管理制度、策略）
	*行业特色技能：计算机取证	信息系统取证	1. 信息安全法规 2. 信息系统取证方法、手段与工具使用	*计算机取证
	*行业特色技能：电子商务系统安全	1. 电子商务系统安全方案设计 2. 电子商务系统安全管理维护	1. 电子商务应用基础 2. 网上安全支付系统	*电子商务安全
安全产品营销与服务	安全产品营销与服务	安全产品营销包括： 1. 客户应用系统的安全风险分析 2. 用户系统安全风险防范方案简单设计 3. 安全产品推介方案、文档策划编写 4. 安全产品演示、讲解 安全产品服务包括： 1. 安全产品安装、使用培训 2. 安全产品故障响应咨询 3. 简易安全产品故障排除	1. 信息及网络安全基础 2. 软件开发基础 3. 硬件开发基础 4. 市场营销 5. 技术支持技巧	1. 信息安全导论 2. 网络安全与管理 3. 信息安全产品与方案 4. 信息安全标准与法规 5. 信息安全产品服务与营销

注：* 为拓展课程。

基于以上分析，根据网络与信息安全学科体系的特点，在注重学生的“动手实践和技能专业化”职教原则的指导下，我们选定《信息安全标准与法规》、《网络攻击与防护技术》、《计算机病毒防护》、《网络及信息安全综合实验教程》、《信息安全产品与方案》、《信息安全管理与工程》等作为“灵创职业教育·网络与信息安全”系列教材的首批丛书。

从学科体系角度看，这些教材构成了下图所示网络与信息安全职业教育体系主体：

法律	技术与开发	管理
	产品与系统	
	评测与服务	
	使用与集成	
	营销与维护	
	培训与认证	

下表为以上课程教学参考学分。

专业课程名称	建议学分	学分分配	
		讲课	课内实验
信息安全标准与法规	4	2	2
信息安全导论	4	2	2
网络攻击与防护技术	5	3	2
计算机病毒防护	4	2	2
网络安全与管理	5	3	2
网络与信息安全综合实验	4	1	3
信息安全产品与方案	4	2	2
信息安全管理与工程	4	2	2
计算机取证与应急响应	3	2	1
合　计	37	19	18

为确保该套教材的质量，教材编委会由国内著名信息安全专家为主组成，每本教材尽可能由经验丰富的职业教育专家执笔。本套丛书主要定位在开设信息安全类专业的职业院校的教材、相应领域的社会培训教材、从业技术人员自学教材。教材既可适用于全国职业教育信息安全专业学生，又可适用于各类成人自考学生。

本套教材受到了国家 973 项目(2007CB311203，2007CB310704)、教育部高等学校博士学科点专项科研基金资助课题(20070013007，20070013005)、国家自然科学基金与香港研究资助局联合科研基金项目(No. 60731160626)和高等学校学科创新引智计划(No. B08004)的资助，在此特表感谢。

杨义先

教授、博导、长江学者特聘教授

2008 年 3 月

前　言

为了引导高等职业技术学校和高等专科学校信息安全相关专业的学生对计算机病毒原理与防治方面所涉及的知识有一个全面的了解，作者编写了《计算机病毒防护》这本书。本教材全面地介绍了目前计算机里常见的病毒及其防治方法。

在讲解时，可以根据所要教的学生对象来选择要教的内容以及内容的深度。对于那些没有学过计算机网络课的学生，可以在课前适当加一些计算机网络、信息安全方面的知识。

本书内容全面，书中内容共9章。第1章是计算机病毒概述，主要包括计算机病毒的产生与发展、计算机病毒的基本概念、计算机病毒的分类；第2章是计算机病毒的工作机制，主要包括计算机病毒的寄生与引导、计算机病毒的传染、计算机病毒的触发机制、计算机病毒的破坏机制、计算机病毒的传播途径；第3章是计算机病毒的表现，主要包括计算机病毒发作前的表现、计算机病毒发作时的表现、计算机病毒发作后的表现；第4章是计算机病毒的发展趋势及特点和技术，主要包括计算机病毒的发展趋势、计算机病毒发展的主要特点、计算机病毒的主要技术、计算机病毒隐藏技术、计算机病毒的变形、计算机病毒新技术；第5章是计算机病毒检测技术，主要包括计算机病毒检测技术的发展历程、计算机病毒检测技术原理、计算机病毒主要检测技术和特点、计算机病毒检测技术的发展方向；第6章是典型计算机病毒的原理、防范和清除，主要包括计算机病毒防范和清除的基本原则和技术、引导区计算机病毒、文件型病毒、文件与引导复合型病毒、脚本病毒、宏病毒、特洛伊木马病毒、蠕虫病毒、黑客型病毒、后门病毒、压缩文件病毒、安全建议；第7章是防范恶意代码技术，主要包括恶意代码的定义、恶意代码的处理；第8章是常用防病毒软件，主要包括防病毒产品的发展、常见防病毒产品、防病毒产品的选择；第9章是中国计算机病毒法律与制度建设，主要包括计算机病毒的法律问题、计算机病毒防范管理制度建设。本书第1、6、7、8、9章及附录由北京电子科技职业学院刘正宏老师编写，第2、3、4、5章由北京邮电大学计算机科学与技术学院李剑副教授和北京中医药大学信息

中心沈俊辉老师联合编写。

感谢北京邮电大学信息安全中心杨义先教授、钮心忻教授、罗群副教授、徐国爱副教授、张茹副教授、崔宝江副教授、谷利泽副教授、李辉副教授、周亚健博士、辛阳副教授、郑康锋博士、李丽香副教授、杨榆博士、张淼博士、黄正权博士、郑世慧博士、王励诚博士等，他们对本书的出版提出了宝贵的意见和建议。感谢我的博士生导师北京理工大学的曹元大教授，曹老师对于本书的出版给予了极大的支持与帮助。

感谢中国电信研究院的赵阳博士、中科院计算技术研究所的副研究员谭建龙博士、北京交通大学的姚正林博士后，他们对本书的出版给予了很大的支持。其他参与本书审阅编写等工作的还有景博、景绍达、白小梅、李胜斌、陈艳霞、益德全、李美丽、李健保、李建龙、李保民、杨芬珍、李胜武、李磊、李凯、马一帆、胡兰兰等，这里一并谢过！

由于本书作者水平有限，书中疏漏与错误之处在所难免，恳请广大同行和读者指正，我将在下一版中改正。我的电子邮箱是 lijian@bupt.edu.cn。

李　剑

目　　录

第1章 计算机病毒概述

1.1 计算机病毒的产生与发展

计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。在病毒的发展史上，病毒的出现是有规律的，一般情况下一种新的病毒技术出现后，病毒迅速发展，接着反病毒技术的发展会抑制其流传。操作系统进行升级时，病毒也会调整为新的方式，产生新的病毒技术。

1.1.1 计算机病毒的起源

关于计算机病毒的起源到现在为止有几种说法，但还没有一个被人们所普遍确认，也没有实质性的论述予以证明。

1. 科学幻想起源说

1975 年，美国科普作家约翰·布鲁勒尔(John Brunner)写了一本名为“Shock Wave Rider”(《冲击波骑士》)的书，该书第一次描写了在信息社会中，计算机作为正义和邪恶双方斗争的工具的故事。

1977 年，另一位美国科普作家托马斯·丁·雷恩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，并称为计算机病毒。这是世界上第一个幻想出来的计算机病毒。仅仅在 10 年之后，这种幻想的计算机病毒就在世界各地大规模泛滥。

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作用。也许有些人通过这本书才茅塞顿开，并借助于他们对计算机硬件系统及软件系统的深入了解，发现了计算机病毒实现的可能并设计出了计算机病毒。

2. 恶作剧起源说

恶作剧者大都是那些对计算机知识和技术均有兴趣的人，并且特别热衷于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资，或是要报复一下别人或公司。前者是无恶意的，所编写的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。例如，美国 Internet 蠕虫病毒的编写者莫里斯实际上就属于此类恶作剧者，因为在他编写这个旨在

渗透到美国国防部的计算机病毒之时，并没有考虑到这种计算机病毒会给美国带来巨大的损失。而后者则大多是恶意的报复，想从受损失一方的痛苦中获得乐趣，以泄私愤。例如，美国一家计算机公司的一名程序员被辞退后，决定对公司进行报复，离开前向公司计算机系统中输入了一个病毒程序，“埋伏”在公司计算机系统里。结果这个病毒潜伏了5年多才发作，造成整个计算机系统的混乱，给公司造成了巨大损失。

虽然，计算机病毒的起源还不能证据确凿地归结于恶作剧者，但可以肯定，世界上流行的许多计算机病毒都是恶作剧的产物。

3. 游戏程序起源说

十几年前，计算机在社会上还没有得到广泛的普及应用，美国贝尔实验室的程序员为了娱乐，在自己实验室的计算机上编制了吃掉对方程序的程序，看谁先把对方的程序吃光。有人认为这是世界上第一个计算机病毒，但这只是一个猜想。

计算机病毒的产生是一个历史问题，是计算机科学技术高度发展与计算机文明迟迟得不到完善两者间不平衡发展的结果，它充分暴露了计算机信息系统本身的脆弱性和安全管理方面存在的问题。如何防范计算机病毒的侵袭已成为信息安全领域上亟待解决的重大课题。

1.1.2 计算机病毒发展背景

计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。它产生的背景如下。

(1) 计算机病毒是计算机犯罪的一种新的衍化形式

计算机病毒是高技术犯罪，具有瞬时性、动态性和随机性。它不易取证，风险小破坏大，从而刺激了犯罪意识和犯罪活动，是某些人恶作剧和报复心态在计算机应用领域的表现。

(2) 计算机软硬件产品的脆弱性是根本的技术原因

计算机是电子产品，数据在输入、存储、处理、输出等环节中，容易误入、篡改、丢失、作假和破坏；程序易被删除、改写；计算机软件设计的手工方式，效率低下且生产周期长；人们至今没有办法事先了解一个程序有没有错误，只能在运行中发现、修改错误，且不知道还有多少错误和缺陷隐藏在其中。这些脆弱性就为病毒的侵入提供了方便。

(3) 微机的普及应用是计算机病毒产生的必要环境

随着微机的普及应用，计算机病毒迅速蔓延。微机的广泛普及，操作系统简单明了，软硬件透明度高，基本上没有什么安全措施，能够透彻了解它内部结构的用户日益增多，对其存在的缺点和易攻击处也了解得越来越清楚，不同的目的可以做出截然不同的选择。

1.1.3 计算机病毒发展历史

1983年11月3日，一位南加州大学的学生弗雷德·科恩(如图1.1所示)在UNIX系统下，写了一个会引起系统死机的程序，但是这个程序并未引起一些教授的注意与认同。科恩为了证明其理论而将这些程序以论文发表，在当时引起了不小的震撼。科恩的程序，让计算机病毒具备破坏性的概念具体成形。

图1.1 费雷德·科恩

不过，这种具备感染与破坏性的程序被真正称为“病毒”，则是在两年后的一本《科学美国人》的月刊中。一位叫作杜特尼(A. K. Dewdney)的专栏作家在讨论“磁芯大战”