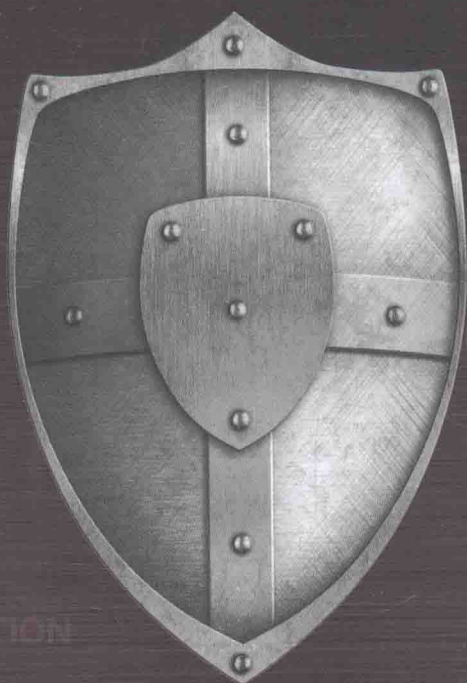




“十二五”普通高等教育本科国家级规划教材
21世纪高等教育信息安全系列规划教材



计算机病毒 原理与防范

(第2版)

秦志光 张凤荔◎主编



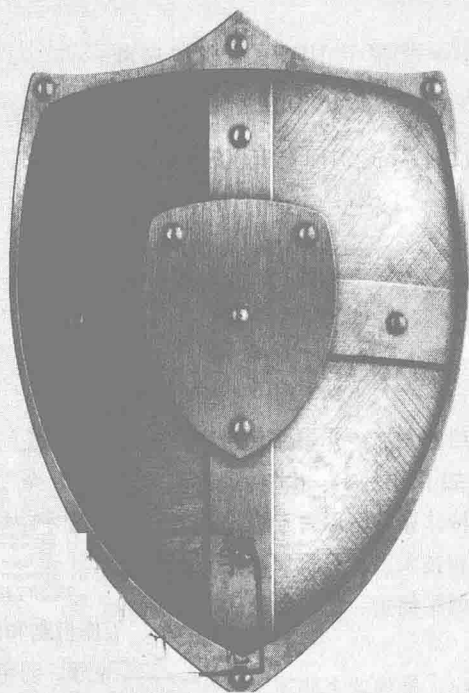
中国工信出版集团



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 and 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

主 任： 方滨兴（院士）

副主任： 贾 焰 马建峰 李凤华 杨义先 张立科

编 委： 马春光 王丽娜 王良民 朱建明 许 进

孙东红 李舟军 李 晖 李建华 李欲晓

吴晓平 邹文波 邹德清 张小松 张红旗

张宏莉 陈晓桦 封化民 胡昌振 俞能海

姚志强 翁 健 谢冬青

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 and 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峒老师完成了第 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	1
1.1 计算机病毒的产生与发展	1
1.1.1 计算机病毒的起源	1
1.1.2 计算机病毒发展背景	2
1.1.3 计算机病毒发展历史	4
1.1.4 计算机病毒的演化	7
1.2 计算机病毒的基本概念	8
1.2.1 计算机病毒的生物特征	8
1.2.2 计算机病毒的生命周期	9
1.2.3 计算机病毒的传播途径	10
1.2.4 计算机病毒发作的一般症状	10
1.3 计算机病毒的分类	11
1.3.1 计算机病毒的基本分类——一般分类方法	11
1.3.2 按照计算机病毒攻击的系统分类	12
1.3.3 按照计算机病毒的寄生部位或传染对象分类	13
1.3.4 按照计算机病毒的攻击机型分类	13
1.3.5 按照计算机病毒的链接方式分类	14
1.3.6 按照计算机病毒的破坏情况分类	14
1.3.7 按照计算机病毒的寄生方式分类	15
1.3.8 按照计算机病毒激活的时间分类	15
1.3.9 按照计算机病毒的传播媒介分类	15
1.3.10 按照计算机病毒特有的算法分类	16
1.3.11 按照计算机病毒的传染途径分类	16
1.3.12 按照计算机病毒的破坏行为分类	17
1.3.13 按照计算机病毒的“作案”方式分类	18
1.3.14 Linux 平台下的病毒分类	19
1.4 互联网环境下病毒的多样化	20
1.4.1 网络病毒的特点	20
1.4.2 即时通信病毒	22
1.4.3 手机病毒	22
1.4.4 流氓软件	23
习题	24

第2章 传统计算机病毒的工作机制及发作表现	25
2.1 计算机病毒的工作步骤分析	25
2.1.1 计算机病毒的引导模块	26
2.1.2 计算机病毒的感染模块	26
2.1.3 计算机病毒的表现模块	26
2.2 计算机病毒的引导机制	27
2.2.1 计算机病毒的寄生对象	27
2.2.2 计算机病毒的寄生方式	28
2.2.3 计算机病毒的引导过程	28
2.3 计算机病毒的传染机制	29
2.3.1 计算机病毒的传染方式	29
2.3.2 计算机病毒的传染过程	30
2.3.3 系统型计算机病毒传染机理	31
2.3.4 文件型计算机病毒传染机理	31
2.4 计算机病毒的触发机制	32
2.5 计算机病毒的破坏机制	33
2.6 计算机病毒的传播机制	33
2.7 计算机病毒发作前的表现	34
2.8 计算机病毒发作时的表现	38
2.9 计算机病毒发作后的表现	42
习题	44
第3章 新型计算机病毒的发展趋势及特点和技术	45
3.1 新型计算机病毒的发展趋势	45
3.1.1 计算机病毒的发展趋势	45
3.1.2 近年主要流行的计算机病毒	48
3.2 新型计算机病毒发展的主要特点	48
3.2.1 新型计算机病毒的主要特点	49
3.2.2 基于“Windows”的计算机病毒	51
3.2.3 新型计算机病毒的传播途径	53
3.2.4 新型计算机病毒的危害	56
3.2.5 电子邮件成为计算机病毒传播的主要媒介	59
3.2.6 新型计算机病毒的最主要载体	59
3.3 新型计算机病毒的主要技术	64
3.3.1 ActiveX 与 Java	64
3.3.2 计算机病毒的驻留内存技术	65
3.3.3 修改中断向量表技术	67
3.3.4 计算机病毒隐藏技术	68

3.3.5 对抗计算机病毒防范系统技术	75
3.3.6 技术的遗传与结合	75
3.4 网络环境下计算机病毒的特点探讨	75
3.5 计算机网络病毒的传播方式	77
3.6 计算机网络病毒的发展趋势	77
3.7 云安全服务将成为新趋势	79
习题	80
第4章 计算机病毒检测技术	81
4.1 计算机反病毒技术的发展历程	81
4.2 计算机病毒检测技术原理	82
4.2.1 计算机病毒检测技术的基本原理	82
4.2.2 检测计算机病毒的基本方法	83
4.3 计算机病毒主要检测技术和特点	83
4.3.1 外观检测法	84
4.3.2 系统数据对比法	84
4.3.3 病毒签名检测法	87
4.3.4 特征代码法	87
4.3.5 检查常规内存数	89
4.3.6 校验和法	90
4.3.7 行为监测法(实时监控法)	91
4.3.8 软件模拟法	92
4.3.9 启发式代码扫描技术	93
4.3.10 主动内核技术	97
4.3.11 病毒分析法	98
4.3.12 感染实验法	99
4.3.13 算法扫描法	101
4.3.14 语义分析法	101
4.3.15 虚拟机分析法	104
4.4 计算机网络病毒的检测	107
4.5 计算机病毒检测的作用	107
4.6 计算机病毒检测技术的实现	108
习题	108
第5章 典型计算机病毒的原理、防范和清除	111
5.1 计算机病毒的防范和清除的基本原则与技术	111
5.1.1 计算机病毒防范的概念和原则	111
5.1.2 计算机病毒预防基本技术	112
5.1.3 清除计算机病毒的一般性原则	113

5.1.4	清除计算机病毒的基本方法	113
5.1.5	清除计算机病毒的一般过程	114
5.1.6	计算机病毒预防技术	115
5.1.7	计算机病毒免疫技术	116
5.1.8	漏洞扫描技术	119
5.1.9	实时反病毒技术	120
5.1.10	防范计算机病毒的特殊方法	121
5.2	引导区计算机病毒	122
5.2.1	原理	123
5.2.2	预防	124
5.2.3	检测	124
5.2.4	清除	125
5.3	文件型计算机病毒	125
5.3.1	原理	125
5.3.2	预防	127
5.3.3	检测	128
5.3.4	清除	131
5.3.5	“CIH” 计算机病毒	131
5.4	文件与引导复合型计算机病毒	135
5.4.1	原理	135
5.4.2	“新世纪” 计算机病毒的表现形式	136
5.4.3	“新世纪” 计算机病毒的检测	136
5.4.4	“新世纪” 计算机病毒的清除	136
5.5	脚本计算机病毒	137
5.5.1	原理	137
5.5.2	检测	141
5.5.3	清除	141
5.6	宏病毒	142
5.6.1	原理	143
5.6.2	预防	145
5.6.3	检测	146
5.6.4	清除	147
5.7	特洛伊木马病毒	147
5.7.1	原理	148
5.7.2	预防	154
5.7.3	检测	155
5.7.4	清除	157
5.8	蠕虫病毒	157
5.8.1	原理	158

5.8.2 预防	160
5.8.3 清除	161
5.9 黑客型病毒	162
5.10 后门病毒	164
5.10.1 原理	164
5.10.2 “IRC” 后门病毒	165
5.10.3 密码破解的后门	167
5.11 不同操作系统环境下的计算机病毒	168
5.11.1 32 位操作系统环境下的计算机病毒	168
5.11.2 64 位操作系统环境下的计算机病毒	169
5.12 压缩文件病毒	170
5.13 安全建议	171
习题	172
第 6 章 网络安全	173
6.1 网络安全概述	173
6.1.1 网络安全的概念	173
6.1.2 网络安全面临的威胁	174
6.1.2 网络安全防范的内容	175
6.2 Internet 服务的安全隐患	177
6.2.1 电子邮件	177
6.2.2 文件传输 (FTP)	178
6.2.3 远程登录 (Telnet)	178
6.2.4 黑客	179
6.2.5 计算机病毒	179
6.2.6 用户终端的安全问题	179
6.2.7 用户自身的安全问题	180
6.2.8 APT 攻击	180
6.3 垃圾邮件	181
6.3.1 垃圾邮件的定义	181
6.3.2 垃圾邮件的危害	181
6.3.3 追踪垃圾邮件	182
6.3.4 电子邮件防毒技术	182
6.4 系统安全	184
6.4.1 网络安全体系	184
6.4.2 加密技术	185
6.4.3 黑客防范	189
6.4.4 安全漏洞库及补丁程序	192
6.5 恶意代码的处理	193

6.5.1 恶意代码的种类	193
6.5.2 恶意代码的传播手法	195
6.5.3 恶意代码的发展趋势	195
6.5.4 恶意代码的危害及其解决方案	196
6.5.5 网页的恶性修改	198
6.6 网络安全的防范技巧	198
6.7 用户对计算机病毒的认识误区	203
习题	205
第7章 系统漏洞攻击和网络钓鱼	206
7.1 系统漏洞	206
7.2 Windows 操作系统漏洞	206
7.3 LINUX 操作系统的已知漏洞分析	210
7.4 漏洞攻击计算机病毒背景介绍	215
7.5 漏洞攻击计算机病毒分析	221
7.5.1 “冲击波”病毒	221
7.5.2 “振荡波”病毒	222
7.5.3 “震荡波”与“冲击波”病毒横向对比与分析	223
7.5.4 “红色代码”病毒	224
7.5.5 “Solaris”蠕虫	225
7.5.6 “震网”病毒	225
7.5.7 APT 攻击	228
7.6 针对 ARP 协议安全漏洞的网络攻击	231
7.6.1 同网段 ARP 欺骗分析	232
7.6.2 不同网段 ARP 欺骗分析	233
7.6.3 ARP 欺骗的防御原则	233
7.7 针对系统漏洞攻击的安全建议	234
7.8 网络钓鱼背景介绍	238
7.9 网络钓鱼的手段及危害	239
7.9.1 利用电子邮件“钓鱼”	240
7.9.2 利用木马程序“钓鱼”	240
7.9.3 利用虚假网址“钓鱼”	240
7.9.4 假冒知名网站“钓鱼”	240
7.9.5 其他钓鱼方式	240
7.10 防范网络钓鱼的安全建议	241
7.10.1 金融机构的网上安全防范措施	241
7.10.2 对于企业和个人用户的安全建议	242
习题	243

第 8 章 即时通信病毒和移动通信病毒分析	245
8.1 即时通信病毒背景介绍	245
8.1.1 即时通信	245
8.1.2 主流即时通信软件简介	246
8.1.3 即时通信软件的基本工作原理	249
8.2 即时通信病毒的特点及危害	252
8.3 即时通信病毒发作现象及处理方法	254
8.4 防范即时通信病毒的安全建议	256
8.5 移动通信病毒背景介绍	258
8.5.1 移动通信病毒的基本原理	259
8.5.2 移动通信病毒的传播途径	260
8.5.3 移动通信病毒的危害	261
8.5.4 移动通信病毒的类型	263
8.6 移动通信病毒的发作现象	264
8.6.1 破坏操作系统	264
8.6.2 破坏用户数据	265
8.6.3 消耗系统资源	265
8.6.4 窃取用户隐私	265
8.6.5 恶意扣取费用	266
8.6.6 远程控制用户手机	266
8.6.7 其他表现方式	267
8.7 典型移动通信病毒分析	267
8.7.1 移动通信病毒发展过程	267
8.7.2 典型手机病毒——手机支付病毒	269
8.7.3 手机病毒的传播和威胁趋势	271
8.7.4 手机反病毒技术的发展趋势	273
8.8 防范移动通信病毒的安全建议	274
习题	275
第 9 章 常用反计算机病毒软件	276
9.1 国内外反计算机病毒行业发展历史与现状	276
9.1.1 反计算机病毒软件行业的发展历程	276
9.1.2 国内外反计算机病毒软件行业所面临的严峻形势	278
9.2 使用反计算机病毒软件的一般性原则	282
9.2.1 反计算机病毒软件选用准则	282
9.2.2 使用反计算机病毒软件的注意要点	282
9.2.3 理想的反计算机病毒工具应具有的功能	283
9.3 部分反计算机病毒工具简介	283

9.3.1 瑞星杀毒软件 V16	284
9.3.2 腾讯电脑管家	285
9.3.3 360 杀毒软件	286
9.3.4 诺顿网络安全特警	286
9.3.5 McAfee VirusScan	287
9.3.6 PC-cillin	288
9.3.7 卡巴斯基安全部队	289
9.3.8 江民杀毒软件 KV2011	290
9.3.9 金山毒霸 2011	292
9.3.10 微点杀毒软件	293
9.3.11 小红伞个人免费版	294
9.3.12 ESET NOD32 杀毒软件	295
9.3.13 BitDefender (比特梵德) 杀毒软件	295
9.3.14 微软免费杀毒软件 Microsoft Security Essentials (MSE)	295
9.3.15 Comodo 免费杀毒软件 (科摩多, 俗称“毛豆”)	296
9.3.16 avast! 免费杀毒软件	296
习题	297
附录 计算机病毒原理与防范实验	298
附 1.1 实验 1 PE 文件格式的分析和构造	298
附 1.1.1 实验目的	298
附 1.1.2 实验要求	298
附 1.1.3 实验环境	298
附 1.1.4 实验相关基础知识	298
附 1.1.5 实验过程	302
附 1.2 实验 2 PE 文件的加载、重定位和执行过程	310
附 1.2.1 实验目的	310
附 1.2.2 实验要求	310
附 1.2.3 实验环境	310
附 1.2.4 实验相关基础知识	310
附 1.2.5 实验步骤	310
附 1.2.6 重定位自己的 EXE	312
附 1.2.7 自己加载自己的 EXE 和一个自己的 DLL	313
附 1.2.8 部分程序代码	316
附 1.3 实验 3 脚本病毒的分析	323
附 1.3.1 实验目的	323
附 1.3.2 实验要求	324
附 1.3.3 实验环境	324
附 1.3.4 实验原理	324

附 1.3.5 实验步骤	324
附 1.4 实验 4 蠕虫病毒的分析	327
附 1.4.1 实验目的	327
附 1.4.2 实验要求	327
附 1.4.3 实验环境	327
附 1.4.4 实验原理	327
附 1.4.5 实验步骤	328
附 1.5 实验 5 木马机制分析和木马线程注入技术	331
附 1.5.1 实验目的	331
附 1.5.2 实验要求	332
附 1.5.3 实验环境	332
附 1.5.4 实验原理	332
附 1.5.5 实验步骤	334
附 1.6 实验 6 反计算机病毒软件的功能和性能分析	335
附 1.6.1 实验目的	335
附 1.6.2 实验要求	335
附 1.6.3 实验环境	335
附 1.6.4 实验原理	335
附 1.6.5 实验步骤	335
参考文献	337

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)、