高等学校计算机专业规划教材

计算机安全

赵一鸣　朱海林　孟　愍　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

高等学校计算机专业规划教材

计算机安全

赵一鸣　朱海林　孟　魁　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书研究和讨论计算机安全的理论技术。主要涉及计算机病毒的防治、黑客攻击的预防，特别是介绍了在网络安全和电子商务中应用广泛的信息加密技术。

全书共 8 章。第 1 章是计算机安全概述。第 2,3 两章，介绍计算机病毒的防治，包括计算机病毒概念，典型病毒分析，宏病毒与计算机网络病毒的防治。第 4 ~ 6 章，介绍信息加密技术及其应用，包括：密码学概述；加密算法，涉及 DES 和高级加密标准 Rijndael 算法、RSA 加密算法和椭圆曲线加密算法；密码应用，涉及数字签名协议、身份识别协议和散列函数，并介绍和讨论了 CA 和 PKI 技术。第 7,8 两章，主要介绍网络安全技术，包括网络安全与防范，Web 安全。

本书可作为大学计算机科学与技术和其他有关专业的教材，也可作为信息技术工作者的参考书。

图书在版编目(CIP)数据

计算机安全/赵一鸣等编著. —北京：电子工业出版社，2003.7
高等学校计算机专业规划教材
ISBN 7-5053-8600-X

Ⅰ. 计… Ⅱ. 赵… Ⅲ. 电子计算机—安全技术—高等学校—教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2003)第 019221 号

责任编辑：陈晓莉　　特约编辑：李双庆
印　　刷：北京四季青印刷厂
出版发行：电子工业出版社　http://www.phei.com.cn
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787 × 1 092　1/16　印张：13　字数：333 千字
版　　次：2003 年 7 月第 1 版　2003 年 7 月第 1 次印刷
印　　数：5 000 册　定价：20.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。
联系电话：(010)68279077

《高等学校计算机专业规划教材》

编委会名单

出 版 说 明

为了适应我国21世纪计算机各类人才的需要，根据计算机学科技术发展的总趋势，结合我国高等学校教育工作的现状，立足培养的学生能跟上国际计算机学科技术发展水平，原“全国高校计算机专业教学指导委员会”、“中国计算机学会教育委员会”的大部分专家、教授于2001年4月在上海召开研讨会，参照IEEE和ACM计算机教程2001大纲组织编写与其配套的22种教材，现推荐给国内的院校，作为教学之用。

为了使这套教材体现现代计算机教学的特点，编出特色，来自上海交通大学、复旦大学、国防科技大学、哈尔滨工业大学、华东师范大学、东南大学、华东理工大学、上海大学、福州大学、重庆大学、东华大学等十几所大学的专家、教授成立了以陈火旺院士为主任委员的编写委员会，并多次集中开会，深入讨论了结合我国高等学校计算机本科教育的实际而推出的“93教程”的教学情况，以及由全国高校计算机专业教学指导委员会、中国计算机学会教育委员会提出的《2000计算机学科教学计划》征求意见稿，在研究、学习、借鉴2000年6月ACM和IEEE/CS联合专题组发表的“Computing curricula 2001”报告的基础上，结合当前计算机技术飞速发展的现实——对计算机学科的教学内容不断提出更新的要求，特别是为了全面推进素质教育，以及培养学生的创新精神和实践能力，提出了新的编写思路，使这套教材的知识点能反映当前计算机学科技术发展的前沿和趋势。

ACM和IEEE 2001教程的思想是将计算机学科领域的知识分解为几个主要的核心科目（算法与数据结构、计算机体系结构、人工智能与机器人学、数据学与信息检索、人机通信、数值计算、操作系统、程序设计语言、图形学、可视化、多媒体、网络计算、软件工程）并作为学科的公共要求：对计算机学科的教学要突出理论、抽象和设计三个环节，并强调教学一定要与社会需求相结合。另外，还提出了贯穿于计算机学科中常出现的基本概念，并将这些概念在教材中予以清晰的介绍，灵活的应用，以更好地帮助学生，使之成为一个优秀的计算机工作者。

为了保证这套教材的审编和出版质量，以陈火旺院士为主任委员的教材编委会的专家教授们在2001年4月召开了全体编委、作者讨论会，制订了编写要求和编审程序。编委们对所有教材的编写提纲进行了讨论，对教材的质量做了专门的要求，并设立专门的负责人选。参加这套教材的编审者都是来自全国重点高校、在计算机领域从事教学和科研的专家和学者，他们具有丰富的教学经验，严谨的治学态度，较高的学术水平。

这套教材的出版得到电子工业出版社的积极支持。他们把这套教材列为重点图书出版，并制定了专门的编审出版规定和出版流程，组织了专门的编辑力量和协调机构。

我们希望这套教材的出版，对我国的计算机教育事业的发展做出应有的贡献。

编委会

2003年1月

编 者 的 话

随着计算机技术的迅速发展，计算机日益深入社会各个方面。作为现代科学、军事、经济、工农业生产、交通、通信、教育卫生等领域的高科技手段，计算机在为社会经济的飞跃发展、社会教育的普及提高创造十分有益条件的同时，也潜伏着严重的不安全性、危险性及脆弱性。自20世纪80年代以来，利用计算机进行高技术犯罪的事件不断出现，计算机安全，或者更全面的是信息安全已成为人们关注的问题。

计算机的不安全因素来自诸多方面，例如自然的、环境的、管理的、计算机软件的、硬件的以及各种人为的因素。所以，计算机安全除了与计算机本身的各个学科，如计算机科学、计算机硬件、计算机程序设计、操作系统、数据库、计算机网络等有关外，还与数学、物理、通信、信息管理、密码学、工程技术学，甚至社会科学、人文科学等学科有着密切的联系。

本书系统介绍了与计算机安全有关的基本概念、方法和技术。全书共分 8 章，第 1 章介绍安全的基本概念以及有关计算机安全的法律、法规。第 2 章介绍了计算机病毒概况，包括计算机病毒和反病毒技术的发展概况，以及计算机病毒的基本结构和防治的基本方法。第 3 章通过剖析典型计算机病毒，特别是近年来通过网络传播的病毒，介绍了如何识别、清除和防范计算机病毒的知识及其防治方法。第 4 章介绍了密码学的基本概念，讨论了古典密码的加密方法和分析方法，并介绍了 Shannon 的密码学理论，简单介绍了序列密码的基本概念。第 5 章介绍了现代加密算法，包括对称密码算法和公开密钥密码算法，介绍了数据加密标准 DES 算法和高级数据加密标准 Rijndael 算法，以及公钥密码算法 RSA、ElGamal 和椭圆曲线加密算法。第 6 章介绍了密码技术在信息安全中的应用，包括数字签名和身份认证，并讨论了 CA 和公钥密码基础实施(PKI)。第 7 章介绍了网络攻击与防范概念，包括网络系统存在的安全漏洞、黑客攻击策略、防火墙技术和入侵检测技术。第 8 章介绍了 Web 安全问题，包括 Web 所面临的安全威胁和防范技术，并讨论了电子商务安全。本书可作为大学本科计算机专业的计算机安全和信息安全课程的教材，适合约 54 学时的教学，部分内容可供学生阅读。为了加深对知识的理解，各章都配了一些思考题供读者练习。

本书在作者多年教学实践基础上编写而成。但由于作者的知识和写作水平有限，对于本书中出现的缺点错误，恳请广大读者批评指正。

本书的第 1 章到第 5 章由赵一鸣编写，第 6 章由赵一鸣和朱海林编写，第 7 章和第 8 章由朱海林和孟魁编写。

在本书编写过程中，得到了教材编委会的关心和支持；电子工业出版社负责本书编辑出版工作的全体同仁工作认真，一丝不苟，为本书的出版付出了大量辛勤劳动；本书初稿在复旦大学计算机系教学使用过程中，有关教师和部分学生提出了不少宝贵意见。在此一并表示衷心的感谢！

编　者

2003 年 5 月

目　录

第 1 章　计算机系统的安全性

随着计算技术的发展和计算机的普及，计算机已进入社会生活的各个角落，在金融现代化、企业管理科学化等方面发挥着巨大作用。特别是因特网的推广应用，使得人们逐步改变生活、工作、学习和合作交流环境，走向信息化时代，科学技术、经济和社会将得到新的发展。但是在带来巨大的社会和经济效益的同时，却潜伏着严重的不安全性、危险性及脆弱性。自 20 世纪 80 年代以来，利用计算机进行高技术犯罪的事件不断出现，计算机病毒泛滥成灾，还出现了热衷于攻击计算机系统的计算机爱好者。计算机安全，或者更全面的是信息安全已成为人们关切的问题。

1.1　计算机犯罪及其法律责任

科学技术是一面双刃剑，它既可以极大地造福于人类，同时也可伤害甚至毁灭人类。中国古人发明了火药，却可用来制造枪炮，使得世界各地战火四起，生灵涂炭。而核武器在威胁人类的同时，核能的开发和利用则为人类提供了取之不尽用之不竭的新能源。而计算机从 1946 年诞生起，就开始造福于人类。但利用计算机进行犯罪也随之而起。

利用计算机进行犯罪活动是从 20 世纪 60 年代末开始出现的，在 70 年代发案率迅速上升，80 年代以来已成为各国日益严重的社会问题。

1983 年哥伦比亚发生了一起轰动一时的计算机盗窃案。这年的 5 月 12 日，伦敦的大通银行接到哥伦比亚中央银行的计算机指令：把 1350 万美元过户到纽约的大通银行的一个户头上。次日该款项又从纽约的大通银行过户到纽约的摩根信托保证银行，然后又转到苏黎世的以色列哈普林银行的一个美国人户头上。26 日这笔钱转移到巴拿马的一家银行。因一个同案犯没有正确文件提取现金，这笔钱再一次转到欧洲。此案于 11 月暴露，经 6 个月调查，有 12 人被捕。

日益增长的计算机犯罪活动已构成了对国家安全和防御、政治、经济、科学技术、社会生活的严重破坏和威胁。

1.1.1　计算机犯罪概念

计算机犯罪是一种高技术手段的犯罪活动。从某种意义讲，电脑犯罪是随时随地可以进行的。随着计算机网络的建立和发展，地理上的界限已不能阻挡这些犯罪活动的发生，对于军事系统或金融系统的计算机犯罪分子可以在一个国家内进行针对另外一个国家的破坏活动。

我国有关方面提出的计算机犯罪定义是：以计算机为工具或以计算机资产为对象(包括硬件系统、软件系统和机时、网上资源等)实施的犯罪行为。

当前计算机犯罪主要有以下类型：

① 对程序、数据、存储介质的物理性破坏。

② 窃取或转卖信息资源。

③ 盗用计算机机时。

④ 利用系统中存在的程序或数据错误，进行非法活动。

⑤ 非法进行程序修改活动。

⑥ 信用卡方面的计算机犯罪

1.1.2 计算机犯罪的手段与特点

根据对目前计算机犯罪案例的分析和统计，主要有以下犯罪手段：

① 数据欺骗——在计算机系统中，非法篡改输入/输出数据。

② 特洛伊木马——这种方法是在程序中存放秘密指令，使计算机在仍能完成原先指定任务的情况下，执行非授权的功能。特洛伊木马的关键是采用潜伏机制来执行非授权功能。计算机病毒通常都包括了特洛伊木马功能。

③ 超级冲杀——超级冲杀是一个当计算机停机、出现故障或其他需要人为干预时计算机的系统干预程序。它相当于系统的一把总开关钥匙。如果被非授权用户使用，就构成了对系统的潜在威胁。

④ 活动天窗——这是利用人为设置的窗口侵入系统。通常指故意设置的入口点，通过入口点可以进入大型应用程序或操作系统。在排错、修改和重新启动的时候，可以通过这些窗口访问有关程序，而罪犯则可利用它来寻找系统软件的薄弱环节，进行非法侵入活动。

⑤ 逻辑炸弹——这是插入程序编码，这些编码仅在特定时刻或特定条件下执行，故称为逻辑炸弹或定时炸弹。逻辑炸弹的关键是特定条件下的程序激活。计算机病毒的可激发特征，实际上就是一个逻辑炸弹。

⑥ 浏览——在系统或终端设备上，利用合法使用手段进行搜索或访问非授权文件。例如：在存储区搜索某些有兴趣或有潜在价值的东西，也可利用合法访问系统某一指定部分文件的机会，趁机访问非授权文件，这些都是以正常操作为掩护所进行的非法活动。

⑦ 数据泄露——有意转移或窃取信息的一种手段。

⑧ 冒名顶替——利用窃取用户的口令，冒名窃取信息，或者当一个用户在用口令进入工作状态后临时短暂离开时，被他人以用户身份获取信息或数据。

⑨ 蠕虫——蠕虫是通过网络来扩散错误，进而危害整个系统。在分布式系统中，可通过网络来传播错误，进而造成网络服务发生死锁。通常需要重新启动系统才能排除蠕虫对系统的恶性作用。

⑩ 间接窃取信息——利用统计信息数据推导机密信息。

随着计算机技术的进步，计算机犯罪方式和手段也日趋复杂和多样化，而预防和安全措施还跟不上节奏。在现代生活中，计算机犯罪有下述特点和趋势：

① 罪犯趋向年轻化，目前计算机犯罪的人员平均年龄为 25 岁。

② 罪犯往往是最熟练和有知识的技术人员，往往是掌握核心机密的人。

③ 计算机犯罪采用的手法和正常活动只有很小的偏差。计算机专家进行未授权活动，往往不被制止，进而导致严重的犯罪行为。

④ 计算机犯罪是可在瞬间发生的高技术犯罪，往往不留痕迹，在法律上难以拿到证据。

⑤ 计算机犯罪活动趋向国际化，有的计算机犯罪是在罪犯跑到其他国家之后才实施的。

⑥ 计算机犯罪造成的经济损失巨大，而罪犯往往并不意识到。像制造计算机病毒，如

蠕虫病毒事件，病毒制造者事先并没意识到会造成 6000 多台计算机停机，到后来想制止也无能为力。

1.1.3 有关计算机安全的法律、法规与法律责任

为了有效制止计算机犯罪，从 1986 年起，根据我国实际情况，借鉴国外有益经验，陆续制定了有关计算机安全的标准和法律、法规。目前正式颁布执行的有关计算机信息系统安全的法律、法规和管理条例见表 1.1。

表 1.1 计算机信息系统安全相关法律、法规和管理条例

法律、法规名称	实施日期
计算机软件保护条例	1991 年 6 月 4 日
中华人民共和国计算机信息系统安全保护条例	1994 年 2 月 18 日
中华人民共和国计算机信息网络国际联网管理暂行规定	1996 年 2 月 1 日
中华人民共和国计算机信息网络国际联网管理暂行规定实施办法	1997 年 12 月 8 日
计算机信息系统安全专用产品检测和销售许可证管理办法	1997 年 12 月 12 日
计算机信息网国际联网安全保护管理办法	1997 年 12 月 30 日
商用密码管理条例	1999 年 10 月 7 日
互联网信息服务管理办法	2000 年 9 月 20 日
中华人民共和国电信条例	2000 年 9 月 5 日
全国人大常委会关于网络安全和信息安全的决定	2000 年 12 月 29 日

上述法律、法规对计算机信息系统和国际联网安全保护的内容作了说明和规定，对计算机安全产品的生产、检测和销售规定了具体管理办法，并明确了违反有关法律、法规所应承担的法律责任。

在所颁布的法律、法规中明确规定了对计算机病毒和危害社会公共安全的其他有害数据的防治研究工作，由公安部归口管理；并明确指出国家对计算机信息系统安全专用产品的销售实行许可证制度，安全产品的检测由国家授权的检测中心按照国家标准或有关规定进行检测。

对于非法入侵网站，也将根据所造成的危害依法追究法律责任。此外，任何组织和个人违反有关计算机安全的法律法规，给国家、集体或者他人财产造成损失的，还要依法承担民事责任。如果构成违反治安管理行为，将依照《中华人民共和国治安管理处罚条例》的有关规定处罚。如果侵入国家要害部门的计算机系统，或危害其他计算机系统而造成严重后果，构成犯罪的，将依法追究刑事责任。

对计算机犯罪及应承担的刑事责任，在 1997 年全国人大通过的《刑法》修正案对此也作了规定：对违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的；或者故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行而造成严重后果的，都将追究刑事责任，处三年以下有期徒刑或者拘役。对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行；或者对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，由此造成严重后果的，也要追究刑事责任，处五年以下有期徒刑或者拘役，后果特别严重的，处五年以上有期徒刑。

总之，有关计算机系统的安全条例和法律、法规正在不断制定和完善中，它们对于促进和保障我国计算机产业发展和计算机应用，对于维护国家主权和独立，对于巩固国防和国家经济建设的顺利发展，对于保护公民在数据和信息资源方面的合法权益，都起着重要作用。国家制定和实施有关计算机安全的法律、法规，是希望从事计算机研究、开发、应用的人们和计算机爱好者能够有章法可依，对计算机系统有害的事不做，防止不安全因素对计算机系统可能引起的破坏。计算机系统的建设者和应用者都应当遵守国家的法律法规，共同维护计算机系统的安全。

1.2 计算机系统的安全性

计算机系统的安全性具有丰富的内容，包括的内容很广，尚没有一个对计算机系统安全性的统一定义。但一般来说，计算机安全是指计算机系统有保护、没有危险，即计算机系统的硬件、软件和数据受到保护，不因偶然和恶意的原因而遭到破坏、更改和显露，计算机系统能连续正常运行。

1.2.1 计算机系统安全性的构成

从构成上看，计算机系统的安全性由 4 部分构成：

① 实体安全——包括硬件和外在环境。例如：机房环境，建筑布局，电源连接，硬件布局等都有一定的规范。

② 软件安全——它涉及软件本身可靠性和软件保护。软件本身可靠性包括软件功能是否完善、正确，是否会出现异常，像“千年虫问题”。这些问题可通过软件测试技术加以解决。软件保护包括软件防修改能力和防复制能力。其中防修改能力主要是为了制止计算机犯罪，防篡改和复原，这可通过引进信息加密技术予以解决；而防复制能力则是软件制造商关心的怎样防盗版问题，这个问题是相对困难的，因为为了用户使用方便，很难采用一些能有效防盗版的技术。

③ 数据安全——数据安全性主要体现在数据防修改能力(制止犯罪)和数据隐蔽性(防止非法获取信息)上，此外还有数据的异常丢失(这涉及非法删除和病毒破坏)。要指出的是，数据安全与程序安全性是有所区别的。采用信息加密技术，引进签名机制，对保证数据安全有相当的作用。

④ 运行安全——它是指计算机运行过程中的安全性，计算机病毒就是对运行安全的极大威胁。分析病毒机制，找到检测和清除计算机病毒的基本思想，以保证计算机运行安全，是计算机安全十分重要的问题。

1.2.2 加强信息安全，迎接时代挑战

计算机技术和网络技术的发展，使我们已处于信息时代。信息化是目前国际社会发展的趋势，它对于经济、社会的发展都有着重大意义。但一种用信息为武器的战争形式却也随着信息化时代的到来而到来。试想一下，在信息时代，如果你的对手能够方便地攻击你的军事信息网络，国家、政府以及商业的信息网络，能够改变你所要的信息和你所拥有的信息系统，那将会怎样呢？可以说你将无法相信自己所拥有的信息和系统，因为无法确定哪些信息是真的，哪些信息是敌方伪造的，甚至核武器的控制信息也可能被更改，使它可能根本无法

发射，或者就在发射井中爆炸，或帮助敌方毁掉自己的城市。这一切无需发动大规模的常规战争，也不需要宣布战争开始，你的对手就能对你的政治、经济基础和军事目标进行突袭，而导演一出现代的“珍珠港”事件。这就是信息战的一般含义。

所谓信息战是指信息领域中敌我双方争夺信息优势，获取控制信息权的战斗。信息战分为信息防御战和信息攻击战。信息攻击战包括偷窃数据、散播错误信息、否认或拒绝数据存取、从物理上摧毁作为数据存储和分发的部分磁盘及武器平台与设施。信息防御战使用病毒检查、嗅探器、密码和网络安全系统抵御敌方的进攻。

信息战的攻击对象主要是信息，对敌方信息或窃取或更改或破坏，甚至毁坏信息基础设施，可以使对手完全丧失处理信息的能力是信息战的战略目标。海湾战争时期，美军通过攻击伊拉克的军事信息系统，使伊拉克军队指挥失灵、通信中断、兵器失控，部队处于被动挨打的局面，这就是信息攻击的结果，是信息战的雏形。而未来信息战的主要武器将是软件武器、芯片陷阱、电磁窃听、高能射频枪等。

随着人们对计算机和软件依赖性的不断增加，计算机病毒、逻辑炸弹和特洛伊木马对信息系统安全性的危害也不断加深，它们成为信息战的主要武器。特别是计算机病毒对抗的研究就是企图把计算机病毒通过无线电方式、网络方式等，植入到对方，伺机破坏对方武器系统的计算机系统，使他们的计算机在关键时刻受到诱骗或崩溃。

所谓芯片陷阱就是设计者为预定目的而对计算机芯片进行修改或更改集成电路的行为，如可以使芯片有优先接受特定指令的能力，这样只要卫星系统发出命令，就可使使用这些芯片的信息系统发生逻辑错误甚至崩溃。

电磁窃听是指利用电磁窃听装置把对方计算机大量的信息电磁辐射予以复原。

高能射频枪实质上就是一部无线电发射机，它可以对一个电子目标发射大功率无线电信号，使其无法工作，甚至使整个网络系统失灵。另一种摧毁性武器也有可能产生，那就是能量比高能射频枪的大，以光速发射出去的电磁脉冲或信号，其强度大到足以使受攻击的计算机内部元件熔化。选择潜伏或收买在对方系统中工作的人员，利用他们进行收集信息或直接将恶性程序传输到系统中，更是信息战中常会采用的手段。

电磁大轰炸则是科索沃战争采用的手段之一，通过电磁干扰，使得南斯拉夫的防空系统陷于瘫痪状态，无法积极有效应战，处于被动挨炸的地步。

过去的战争是谁拥有最好的武器，谁就可能在战争中取胜。而今天，则是谁掌握了信息控制权，谁就胜利在望。事实上，在当今信息化时代，攻击者只要使得对方的金融系统、证券交易系统以及经济信息统计系统发生问题，就足以使得对方经济发生混乱，甚至濒于崩溃。

我们现在善于接受新的事物，以敏捷的行动不断地拿来，而往往忽视了新事物还伴随挑战、威胁和侵略。因此我们必须重视信息安全，大力发展自己的信息系统安全产品，迎接时代的挑战。

第 2 章　计算机病毒概述

在生物学中，病毒是那些能够侵入动物体并给动物体带来疾病的一种微生物。而计算机病毒则是在计算机之间传输，并自己进行复制而给计算机系统带来一定不良后果的一类程序。计算机病毒是随着计算机软件技术的发展而逐渐产生的，是计算机科学技术高度发展与计算机文明得不到完善这样一种不平衡发展的结果。

2.1　计算机病毒的发生和发展

2.1.1　计算机病毒的起源

考察如今泛滥成灾的计算机病毒，可追溯到科学幻想小说。在 1977 年夏季 Tkomas.J.Ryan 推出了轰动一时的科幻小说，名叫《The Adolescence of P-1》。在这本书中，作者构造了一种神秘的、能自我复制、利用信息通道传播的计算机程序，称为计算机病毒。这些病毒漂泊于电脑之内，游荡于硅片之间，控制了 7000 多台计算机的操作系统，引起混乱和不安。从科幻到大规模泛滥仅用了十多年时间，故有人认为计算机病毒起源于科幻小说。

作为计算机病毒起源的另一种说法是恶作剧说。即一些人为了显示自己的计算机知识方面的天资，或出于报复心理，编写了恶作剧程序，并通过软盘交换特别是游戏盘的交换，引起计算机病毒的广泛传染。此外，也有人认为，软件制造商为了保护自己的软件不被非法复制，而在软件产品中加入病毒程序并在一定条件下触发传染（如非法拷贝）。

不管计算机病毒是怎样起源的，这一点是肯定的，即计算机病毒是随着计算机软件技术的发展而逐渐产生的。其思想来源于早期的特洛伊木马程序（程序开发者开发一个表面上可靠的程序，可是使用者使用一段时间后，便会出现各种问题）。编制这类程序的人一般有两种，一是恶作剧者，他们具有较丰富的系统知识和编程经验，试图通过这种程序来显示自己的才能；其次是心怀不满的报复者，他们在自己开发的软件中加入特洛伊木马，以达到报复目的。后来，随着软件技术的发展，了解系统的人越来越多，他们中间少数人从生物界的某些现象中受到启发，便不断改进自己的特洛伊木马程序，从而衍生出现在的计算机病毒。而软件制造商为了追踪非法复制软件的现象，在软件中加入计算机病毒，则更是对计算机病毒的流行起了推波助澜的作用。

2.1.2　计算机病毒的发展历史

1977 年，在科幻小说中提出了计算机病毒，而到 1983 年，美国计算机安全专家 Fred Cohen 通过实验证明了产生计算机病毒的现实性，制造了世界上第一例计算机病毒。并在 1984 年 9 月的加拿大多伦多国际信息处理联合会计算机安全技术委员会举行的年会上，发表了题为“计算机病毒：原理和实验”的论文。其后，又发表了“计算机和安全”等论文。但这些论文并没有引起新闻界的重视，因为计算机病毒只是在实验室中产生，作为一种研究行为，并没有在社会上产生。