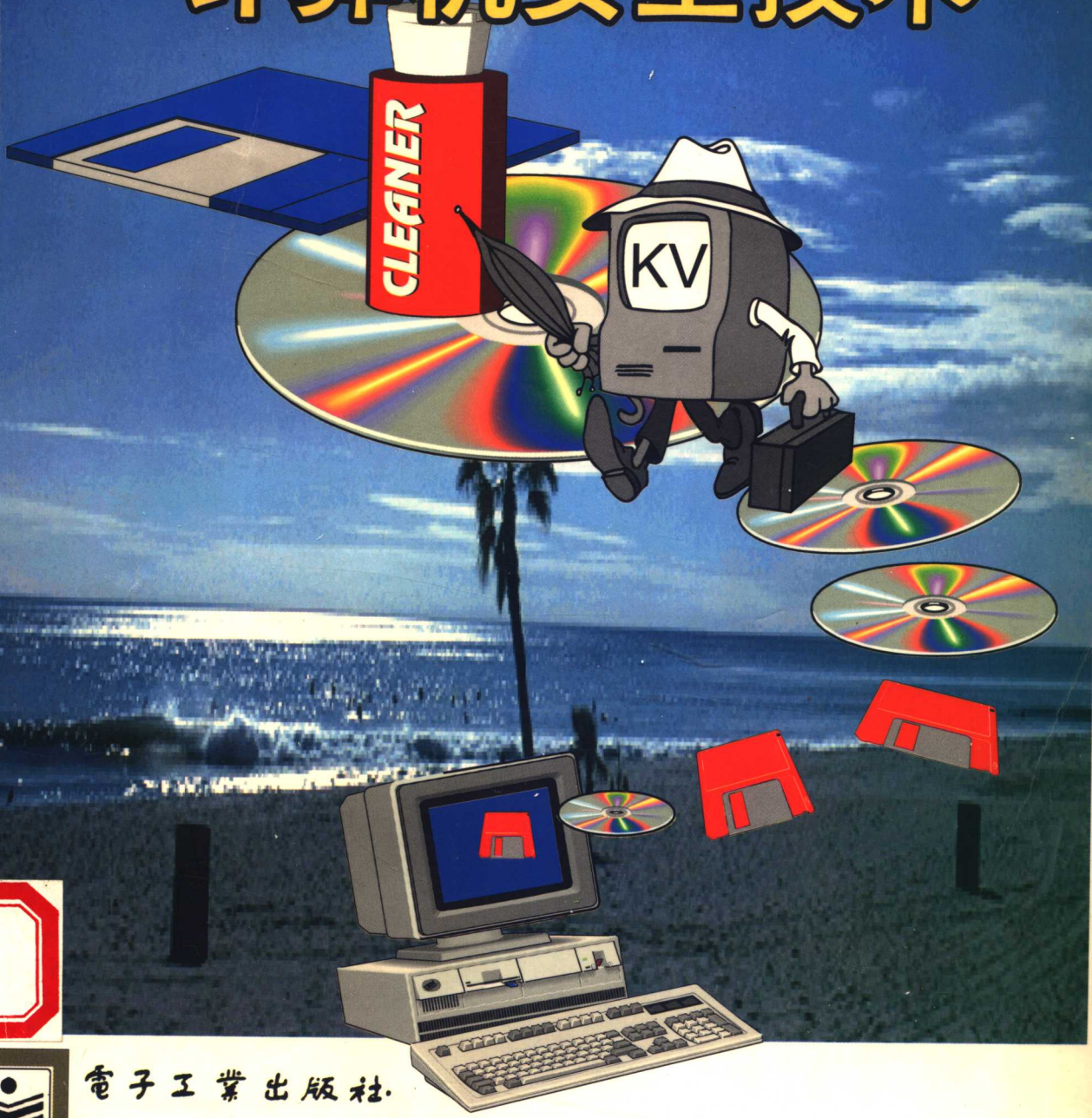
学用电脑 TV 手把手教育工程丛书

中国计算机函授学院教材编写组编写

祝您平安

手把手教您

计算机安全技术



電子工業出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY URL:http://WWW.phei.co.cn

全国二十余家省级以上电视台教学联播
国家863智能计算机主题专家组指导主审
中国计算机函授学院教材编写组编写

学用电脑·TV 手把手教育工程丛书

手把手教您计算机安全技术

作者 殷 伟 张 莉
主编 牛允鹏
主审 汪成为

電子工業出版社
Publishing House of Electronics Industry

内容简介

本书全方位的向读者介绍了计算机安全的概况，特别注重对实际应用、操作技巧、具体方法的指导和示范，真正做到手把手教和学的目的。

可供高等院校计算机专业师生、从事计算机专业应用的工程技术人员、计算机安全管理人员以及广大计算机用户阅读参考。

丛 书 名：学用电脑·TV 手把手教育工程丛书
书　　名：手把手教您计算机安全技术
作　　者：殷　伟　张　莉
责任编辑：吴金生
特约编辑：陈淮民
排版制作：电子工业出版社照排室
印 刷 者：
装 订 者：北京科技印刷厂印刷
出版发行：电子工业出版社出版、发行
北京市海淀区万寿路 173 信箱　邮编　100036　发行部电话：68214070
URL：http://www.phei.co.cn
经　　销：各地新华书店经销
开　　本：787×1092 1/16　印张：13　字数：312 千字
版　　次：1997 年 8 月第 1 版　1998 年 1 月第 2 次印刷
书　　号：ISBN 7-5053-4245-2/TP·1916
定　　价：17.00 元

序

再有不到4年时间，世界经济就要踏入21世纪的门槛。中国经济在21世纪会不会有奇迹？这是每个中国人乃至一切关心中国经济发展的国外人士所共同关注的问题之一。显然，12亿中国人都十分盼望我们自己的国家在新世纪里重新成为世界强国，都在翘首以待国富民强的日子。

站在这世纪之交的路口，党中央及时提出了“科教兴国”的战略。因为“科学技术是第一生产力”，它能够极大地提高经济发展速度，而教育则可以培养大量人才并且能够提高全民的素质，推进科技进步，加速推动经济发展。

21世纪将是信息化社会，这是勿庸置疑的。数十年来信息技术的发展，已在相当程度上直接影响了各国综合实力的变化。当前世界一些国家展开科技的竞争，聚焦点又多集中在信息技术上，投入力量之巨、发展速度之快，令人难以想象。而信息技术尤其是计算机技术，对各个领域包括尖端技术领域的浸透，又是那么全面而彻底。

面对世界新技术革命浪潮的冲击，以及世界各国在信息技术方面的激烈竞争，我国也作出了一系列反映。江泽民总书记曾经指出：“四个现代化，哪一化也离不开信息化。”“八六三”计划所列七个高技术发展重点，其中一个领域就是信息技术。1993年，我国政府又提出并开始实施“三金”工程和“金”字系列工程等一批全国性的重大信息基础设施建设项目。这些都在全世界引起了强烈反响。

我们必须清楚地认识到，信息技术正在迅速影响着国家的教育、人们的生活、工作等方方面面。如今，“多媒体”、“网络计算”、“人工智能”等对人们已不再是陌生的名词，而是触手可及的存在，并且它们正在不断地改变着这个世界。不管我们愿意不愿意，我们都必须去适应信息社会的发展，主动迎接信息社会的挑战。我们只有一种选择，那就是将中国人的智慧融入人类社会的发展，创造出我们新的辉煌。

中国计算机函授学院紧跟社会发展的潮流，多年来在我国大力普及计算机技术，推广计算机应用，做出了令人瞩目的成绩。最近，他们组织实施“学用电脑、电视手把手”教育工程，旨在进一步提高我国的计算机普及应用水平。这一工程包括出一套丛书、在电视台播讲教学课程、出版录相带、VCD、举办一些专项(科)培训班等。这是一个好主意、好举措。

手把手丛书立意新、起点高、选材得当。我看它有两个目标：一个是近期的，即通过大量新技术的普及，使得我国的计算机能够发挥最好的作用和最佳的效益；其二是远期的，使我国21世纪人才具备和信息社会接口的能力，能驾驭计算机及各种信息技术和系统，逐步提高全民的素质。

光靠热情和勇气实现梦想是不可能的，21世纪我国在世界上的地位靠我们自己去争取，脚踏实地、认认真真地为国家做好每件事，那才是最重要的。

汪成为

一九九七年七月

汪成为教授系中国计算机学会副理事长、中国工程院院士。

出版说明

九十年代以来，全球信息技术发展速度明显加快。由于芯片技术、电脑软件技术突飞猛进地提高，电脑功能正日趋强大；随着 Internet(国际互联网络)的出现，二十年前，未来学家所描绘的信息爆炸的时代，已经赫然降临在我们面前。

尽管，世界经济目前还按照后工业化时代所形成的轨迹做着惯性飞行。但是，人们都已认识到，我们周围的一切正在发生异乎寻常的变化。

今天，如果你还在漫不经心的思考问题，安于现状，你就很难获得二十一世纪的入场券！

再仔细地看看我们身边："奔腾"赞歌唱遍各个角落，多媒体计算机迅速走进家庭，WWW 浏览器使你坐在家中如同周游世界，Windows 95、Windows NT、Excel、Java 等新软件层出不穷……

所有这一切，真叫人难以把握！

《手把手》丛书在这样的形势下问世了。显然，她希望在您困惑的时候成为您的朋友，伴您走向变幻无穷的信息时代。

该套丛书一共 20 本，可分为五类：

- 基础类
  - 手把手教您电脑文字处理技术
  - 手把手教您组装与维护电脑
  - 手把手教您使用中文 Windows 95
  - 手把手教您正确使用电脑工具软件
  - 手把手教您计算机安全技术
- 图形处理类
  - 手把手教您用 CorelDRAW 绘画
  - 手把手教您用 Photoshop 处理图象
  - 手把手教您用 AutoCAD 制图
  - 手把手教您用 3DS 制作三维动画
- 实用软件
  - 手把手教您活用电子表格 Excel
  - 手把手教您用 FoxPro 管理数据库
  - 手把手教您方正排版
  - 手把手教您财会电算
  - 手把手教您使用 Word 处理文档
- 网络类
  - 手把手教您使用 Novell 4.xx 网络
  - 手把手教您使用 Windows NT 组网
  - 手把手教您使用国际互联网络 Internet
- 多媒体类
  - 手把手教您用 AuthorWare 制作多媒体软件
  - 手把手教您电脑娱乐与家教
  - 手把手教您操作家用多媒体电脑

该套丛书立足于求新、求精、手把手。

求新：概括目前最新的电脑知识，最新的操作技术，以飨读者。

求精：对现有新知识进行提炼，精选出最经典的、最有用的奉献给读者。

手把手：力求通俗易懂，生动有趣，步步引导，使读者快速掌握。

本套丛书由中国计算机函授学院组织编写，国家 863 智能计算机主题专家组担任丛书指导；全套书由电子工业出版社出版；所配教学录相带将由中国教育电视台和二十余家省级电视台联合播出。

我们期望，这套丛书的出版，将对我国的计算机人才培养起到一定的推动作用，同时也能将我国计算机普及应用水平提高到一个崭新的阶段。

一九九七年六月

祝 你 平 安

（代前言）

20世纪后叶，随着计算机科学技术的飞速发展，特别是计算机的日益普及和计算机网络的广泛应用，使人类社会的工作和生活方式发生了一系列巨大的变化，促进当今社会进入崭新的信息时代。一方面由于计算机系统的开放性和信息共享带来了计算机应用的飞速发展，另一方面也正是这种开放性以及计算机本身安全的脆弱性，导致了计算机安全方面的诸多漏洞。从1966年美国首次对一起篡改银行数据的计算机犯罪案件提出起诉以来到今天，世界范围内的计算机犯罪案件年增长率达30%左右。我国也不例外，截止到1996年底，我国发现计算机犯罪案件已近200起，盗窃钱财从几万到几百万不等，情况十分严重。另外，据公安部门调查表明，我国约有60%的计算机感染过计算机病毒。尤为引人注目的是，计算机病毒已被应用于政治和军事目的，如我国发现的“6·4”计算机病毒就具有极强的政治性和破坏性。特别是今天“Internet”互联网在我国的不断发展，使国外一些反动的、不健康的黄色垃圾传入我国，如果我们不加以控制和管理，其后果不堪设想。

我国在充分重视和研究了发达国家曾走过的弯路——只强调推广计算机应用，而忽视计算机安全的深刻教训后，于1983年就成立了公安部计算机安全监察局，主管全国的计算机安全工作。1994年2月18日国务院发布了《中华人民共和国计算机信息系统安全保护条例》，标志着我国计算机安全工作正逐步走向法制化和科学化的管理轨道。

本人作为公安计算机安全监察人员，通过多年大量的工作实践，现将自己对计算机安全管理的研究成果和体会奉献给大家，希望本书能使你获得收益，如能这样，笔者将会感到极大的欣慰。在此，作者要衷心感谢计算机安全界的同行们，书中引用了他们的部分观点，谨向所有给予本书热情支持和大力帮助的人们一并致谢。

最后，引用一句歌曲的歌名“祝你平安”来表达我对广大计算机用户的衷心祝愿！

编　者

一九九七年五月

目　录

第一章

信息社会中的计算机安全

本章内容提要

- ◆ 计算机在信息社会中的地位
- ◆ 计算机犯罪就在我们身边
- ◆ 计算机病毒的起源和影响
- ◆ 计算机病毒在我国蔓延
- ◆ 计算机病毒的危害和对社会的冲击

§1.1 计算机在信息社会中的地址

众所周知，社会的发展需要信息和信息交流，人们几乎无时无刻不和信息打交道。然而，信息的价值真正被人们所认识还是在今天。据统计，在19世纪，知识和信息每50年翻一番；20世纪初约每30年翻一番；20世纪50年代后期约每10年翻一番；而90年代只需3年就翻一番了。这种信息量的急剧增加，使得用手工方式进行信息处理已不能适应需要，必须要有更先进的科学技术来收集、处理、存储和传输信息。而计算机正是这种技术的杰出代表，它的出现使得信息科学技术有了飞速发展，对社会发展产生了深远的影响。

1.1.1 社会的计算机化向我们走来

计算机技术的高度发展为人类提供了高度的自动化和现代化，计算机网络的不断扩大，迅速地向着国际化方向发展，为人类社会的更高速、更高效、更广泛的信息交流提供了条件，过去人们想象不到的许多事情今天都已经变成了现实。特别是到了90年代，在一些发达国家中，计算机应用已经渗透到政治、经济、军事、科学文化和家庭生活等社会的各个领域，计算机已经成为各发达国家社会生活中的重要工具，实现了社会计算机化，改变着社会生产方式和社会的其它活动方式，朝着社会信息化进军。我国也正在努力发展计算机信息产业，目

前投入使用的大、中、小型计算机已达10万多台，微型机300余万台，而且已经开始建立面向国民经济建设和国防建设的全国性经济、业务和指挥等计算机网络系统。由此可见，社会计算机化的出现，使计算机安全问题也随之提到一个非常重要的地位。

1.1.2 计算机的资产正在形成

随着计算机应用的广泛深入；计算机信息系统日益在整个社会活动中发挥着巨大作用，逐步实现自动指挥与控制、生产、管理、办公自动化。原先由人承担的繁重工作，逐步由计算机代替，生产和工作效率大为提高。计算机信息系统也逐步成为一个国家和政府机构运转的命脉和整个社会活动的支柱。

由此，社会的计算机化产生了一种新的社会资产，即计算机资产。

计算机资产由两大部分构成：

⊙一是计算机信息系统资源，即硬件、软件、实体及其相关文件资料，系统相关配套设备和设施、系统服务，甚至计算机业务工作人员等。系统资源具有相当高的价值和使用价值；

⊙二是计算机信息系统生产和拥有的信息资源，或者叫由系统处理、存储、传输的电子信息资源。包括钱、财、物，以及各种有价值的数据，如统计报表、科学技术资料、计划、决策、秘密文件、情报、公民个人的隐私数据等。

如果说系统资源是国家的重要财富，而信息资源则是国家的重要战略资源。谁拥有它，谁就掌握了战略主动权。由此，我们不论从计算机资产的属性，还是从它的社会价值方面看，都会深刻地认识到计算机安全的重大战略意义。

在计算机问世之初，计算机数量还相当少，计算机被视作一种珍贵的财产，所以如何保证软件技术不被窃用是十分重要的。后来，随着计算机技术的发展，计算机从科学计算的领域中走出来，而成为一种事务处理机。当计算机用于管理和商业后，它便成了直接影响组织的生存及发展的重要财富。

在计算机应用尚由专人管理和以主机为主的集中式网络时代，由于信息的流通受到严格的管制，懂得计算机技术的人又不多，因此，计算机应用只有简单的安全性问题。80年代以后，分布式网络日渐普及，跨国境计算机网络应用逐渐建立起来，计算机程序的设计技术迅速普及到大众，而相对的计算机管理技术、网络中的信息交换控制、程序及资源共享秩序与伦理道德、计算机使用者应遵守的法律及人们的基本的价值观念均未得到同步提高，计算机文化及文明远远滞后于计算机技术的应用，这种情况就为今天的计算机犯罪的产生和发展提供了温床。

由此可见，随着计算机和计算机网络的普及，人类信息资源作为一种社会财富得到充分

合理的利用，这时人类的意识形态也应包括计算机部分，从而就要求与之相适应的制度及组织机构亦应得到相应的发展和完善，如法律、法规、道德及教育等等。

§1.2 计算机犯罪就在我们身边

从以上介绍可知，计算机应用已经渗透到社会的各个方面，许多政府机构、企业、家庭都由计算机系统来贮存文件、管理日常事务、参与决策，这些机构都已经完全计算机化了。

由于计算机信息系统自身的脆弱性，以及一些敌对分子和极端利己的不法之徒的存在，利用计算机进行犯罪活动就不可避免，计算机犯罪就在我们身边。

最早的计算机犯罪开始于40年代末期，也就是开始推广计算机应用之时。首先是在军事领域，然后逐步发展到工程、科学、金融、银行和商业等民用领域。1966年美国首次对一起篡改银行数据的计算机犯罪案件提出起诉，到了70年代中期，发案率迅速上升，80年代以后，世界范围内的计算机犯罪案件年增长率达30%左右，在个别高技术集中地区，如美国硅谷，案发率更高，中国也不例外。由此可见，计算机犯罪正在全球逐渐蔓延并成直线上升趋势。

下面举一起发生在我们身边的计算机犯罪案例，以提醒大家警惕。这是安徽省第一起电脑盗窃案，就发生在合肥市长江路最繁华地段的四牌楼市工商银行营业部。

1.案件发现的经过

1991年12月25日上午，合肥工业大学新技术研究所的会计小沈到市工行营业部办理销户手续。开销户经办人范群查阅该户的余额为54104.83元，而小沈说存款余额应为20504.83元，银行帐上多出33600元！怎么会多出这么多钱来？范群觉得此事有些蹊跷，遂要求小沈待银行核查后再来办理销户手续。随后范群就同营业部负责查帐的潘清查阅了新技术研究所的有关资料、帐页。发现该户的存款余额的确为20504.83元，与研究所来人核对的余额相符，再仔细察看该户资金的来龙去脉，发现这个帐户已很久没有来往的帐目款项，存款余额始终是3.32元，12月17日收到一笔陈旧拖久贷款20497.50元。12月21日帐户收入银行存款利息为33604.11元，总共本金才两万多元，怎么会有3万多元的利息？12月25日该户又转出33600元，付款方是该研究所的帐号，但付款方户名却莫明其妙地变成了“安徽省通信技术公司”，印鉴是“梁恩清”，收款方户名为“钟平商店”，开户行是市百货大楼储蓄所。显然，有人在搞鬼。

27日下午合肥市公安局接到市工行保卫处的报警电话。市刑警队立即组成了由银行保卫处、监察室、会计处、科技处参加的专案组，开始了紧张的侦破工作。他们依据遗留在银

行的“安徽省通信技术公司”印鉴卡,及转往“钟平商店”的转帐发票对案情进行了全面的调查与分析,有关人员提供的情况和一些迹象表明,省工行的陈寅平有重大嫌疑。

2.案发的起因

28岁的陈寅平从一个市工行办公室干事,成为营业部会计股长,继而调入省工行联行科技处对帐中心当科长。他刻苦钻研电脑业务,颇受领导器重(**注意,计算机案件的罪犯往往不少是技术上的尖子**)。有一天,陈寅平正在操作他的计算机,看着显示器上一串串跳动的数字,陈寅平突发奇想:如果能将某一科目中其他储户的积数调整到另一储户上,那么这一储户在电脑计息时定能多计一笔钱,再把这笔计算机误计的利息转到自己另开的帐户上,那么他就可以取得一笔可观的票子,而且其他储户不知道,帐面上的钱也不会少,谁能发现?在金钱的驱使下,一个罪恶的计划在陈寅平脑海中产生。

1991年11月下旬的一个星期天中午,陈寅平来到市工行营业部会计股的一位同志家,谎称自己有些挂历想放在会计股,这位同志见自己原来的老上级来了,现在又是省行对帐中心的科长,便将营业部包括微机房的一大串钥匙给了陈寅平,陈便将一串钥匙全部复制(**注意,管理的漏洞,是促成案发的关键因素**)。12月10日中午12时,陈寅平溜进微机房内,见四下无人便紧张地搜寻计算机密码。熟悉计算机的人都知道,知道了计算机的密码就可以进入计算机系统内改变其信息的内容。然而,茫茫数海,何处寻找?陈逐一试验。无意中发现机子边的桌上玻璃板下放着五张“世界小姐”扑克,按顺次分别是红桃5、红桃Q、方块9、黑桃A、黑桃4,会不会是微机操作员怕忘了密码用五张扑克帮助记忆,陈按50914这个数一操作,正是此密码!(**注意,尽管密码的安全规定,不许用助记数字来作密码,但这种现象却比比皆是,又是一个管理上的漏洞**)12月18日中午,陈用私自配制的钥匙进入机房,进行一次更换软盘的试验性操作,试验成功。随后陈私制了一枚“安徽省通信技术公司”的公章。陈手头又有一个现成的“梁恩清”私章,是一个浙江商人让他代为保管的,于是,一张汇款单位为“安徽省通信技术公司”的印鉴卡伪造成功。12月20日中午,陈又一次溜进市工行营业部,按计划对储户的积数进行调整,使合肥工大新技术研究所的帐上多出了33600元的利息。返回营业大厅,将事先伪造的“安徽省通信技术公司”的印鉴卡放入印鉴卡箱。12月22日下午,陈在其爱人所在的百货大楼储蓄所开了个通存通兑的户名为“钟平商店”的帐户。次日上午,陈将事先填好的付款方为“安徽省通信技术公司”、收款方为“钟平商店”的付款委托书,趁市工行营业部柜台人员转身之际扔入待处理凭证当中。为了掩人耳目,陈在中午操作时,有意把时间改为早晨9:20,而且将自己在计算机上作案的同步打印记录撕毁,以防留下蛛丝马迹。岂料没两天便东窗事发。

由于该案属盗窃未遂,陈作案后在公安机关侦破期间主动投案自首,认罪态度较好,法院依法判处其有期徒刑7年。

电脑盗窃,昨天还作为国外奇闻流传,今天就发生在我们的身边。而且,在破案中出现如此之多的管理和技术上的漏洞这不能不引起管理部门和整个社会的警觉。

§1.3 计算机病毒的起源和影响

计算机病毒的起源,到现在还没有一个为大家所公认的确切说法。尽管如此,对于计算机病毒的发源地,大家都一致认为是美国。

1.计算机病毒的几种起源说

关于计算机病毒的起源现在有几种说法,但还没有一个被人们所确认,也没有实质性的论述予以证明。下面将几种起源说简单介绍一下。

(1)科学幻想起源

1977 年,美国科普作家托马斯·丁·雷恩推出轰动一时的《Adolescence of p - 1》。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,我们不能否认这本书的问世对计算机病毒的产生所起的作用。

(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单位。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 网络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,也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,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,计算机病毒的起源是否归结于恶作剧者还不能够确定,但可以肯定,世界上流行的许多计算机病毒都是恶作剧者的产物。

(3)游戏程序起源说

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,有人认为这是世界上第一个计算机病毒,但这只是一个猜测。

(4)软件商保护软件起源说

计算机软件是一种知识密集的高科技产品,由于人们对于软件资源的保护不尽合理,这就使得许多合法的软件被非法复制的现象极为平常,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拷贝者,而在软件产品之中加入病毒程序并由一定条件触发传染。例如,Pakistani Brain病毒在一定程度上就证实了这种说法。该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,有人认为这是软件制造商为了保护自己的软件不致被非法复制而导致的结果。

2.世界上第一例被证实的计算机病毒

第一例制造计算机病毒的人到底是谁,到目前为止,依然众说纷纭。1983年11月3日,美国计算机专家弗莱德·科恩(Fred Cohen)在美国国家计算机安全会议上,演示了他研制的一种在运行过程中可以复制自身的破坏性程序,伦·艾德勒曼(Len Adleman)将它命名为计算机病毒,并在每周召开一次的计算机安全讨论会上正式提出来,8小时后专家们在VAX11/750计算机系统上运行,第一个病毒实验成功。一周后获准进行实验演示,从而在实验上证实了计算机病毒的存在,这就是世界上第一例被证实的计算机病毒。

可以认为,正像病毒的种类多种多样一样,计算机病毒的产生原因也并非一种。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这样一种不平衡发展的结果,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。

3.计算机病毒的破坏震惊世界

自1983年世界上第一例计算机病毒被专家们在实验中证实以来,直到1987年计算机病毒才开始在世界上广泛传播。可以说在1988年11月前,人们对计算机病毒侵害的反应仍是冷淡的,还不能充分正确地评估计算机病毒所造成的危害。1988年11月2日,美国最大的计算机网络Internet网络遭到计算机病毒的攻击,从此,人们对计算机病毒的认识有了极大的转变,在国际计算机领域掀起一个谈论病毒的高潮。

下面列举一些计算机病毒所造成的危害实例

◉1987年2月美国东部一所医疗中心发生了一桩怪事,存储在医院计算机系统中的全部病历突然莫明其妙地消失了。计算机专家用了很长时间才查明,这是计算机病毒在作怪。编制该病毒的恶作剧者还在计算机中留下了电话号码和这样一句话:"当心病毒,请向我们联系接种疫苗。"

◉1987年12月下旬圣诞节前夕,病毒侵袭了IBM公司的国际电子信息网,恶作剧地先向计算机用户发出节日祝贺,然后根据该系统的用户信息来往名单记录,向每个曾使用过这个信息网的用户发出了相同的贺信,大量连锁信件使得这个著名的大型计算机网络不堪重负而瘫痪,这就是IBM圣诞树病毒。

◎1988 年 3 月 2 日,这天开机工作的所有苹果(APPLE)牌微机在屏幕上自动出现了这样一条信息:"《MacMag》杂志出版商 Richard Brandow 及全体人员,借此机会向全世界所有苹果机用户们转达全球和平信息",接着程序就自行毁坏了。

◎1988 年 9 月 12 日,与日本电气公司联机的日本最大的个人计算机网 PC－VAN 网发生计算机病毒入侵用户计算机事件。

◎1988 年 11 月 2 日,Internet 网络受到计算机病毒的严重攻击,一夜之间造成约 6000 台与该网络系统连接的计算机,包括美国国家航空和航天局、军事基地和主要大学的计算机停止运行的事故,直接经济损失达 9200 多万美元。

◎1989 年 11 月 13 日,星期五,一个被称为"黑色星期五"的恶性病毒在长期潜伏、广泛传播后,在全世界数十万台运行 DOS 的微机上发作。在这天,每运行一个文件,则被删除一个,许多微机用户被迫停机,在全世界范围内造成难以估计的损失。

短短的几年内,计算机病毒就像滚雪球一样,在全世界范围内不断地蔓延,并造成巨大的破坏和无法估计的损失,引起了巨大的恶劣影响。

4.计算机病毒第一次在中国大规模出现

1987 年,面对美国和欧州一些发达国家已经出现计算机病毒的破坏这一情况,我国有关方面已引起注意和警惕,公安部计算机安全监察司告诫人们要警惕计算机病毒的袭击,而我国大多数人却认为国内计算机网络尚处于初期阶段,计算机病毒难以流行起来。但是,事实却和人们的估计相反。1989 年 3 月,我国重庆西南铝加工厂计算中心 7 台计算机无法正常运行,严重影响管理信息系统的运转。经过约一周时间的研究,发现其计算机系统感染上小球病毒,新闻媒介在我国最大的计算机专业报刊《计算机世界》上作了报道,这是我国首例公开报道的计算机病毒,从此拉开了我国探讨和防范计算机病毒的帷幕。

随后,小球病毒在我国迅速蔓延,全国的一些高等学校和科研部门,国家的一些重要机关,北京、上海、广州、天津、江苏等二十一个省、市,甚至计算机使用率不高的边远地区也染上了计算机病毒。受这种计算机病毒侵袭面最大的是国家统计局统计系统的微机,据介绍,这种病毒的来源是 1988 年出自香港的一批 OLIVITTI M－24 微机,其现象是:在计算机屏幕上出现跳动的球状光斑,这些球状光斑无休止地运动,轻则大大减慢计算机的运行速度,重则造成死机,严重影响计算机的正常工作。据公安部计算机安全监察司在全国范围内抽检发现,截至 1989 年底共有 20%的微机感染上这种病毒。以此推算,当时我国约有 6 万多台微机感染上了小球病毒。

一种单一的计算机病毒,从香港传入大陆后,在不长的时间里攻击了大陆数万台微机,在不同层次和不同部门(其中包括政府的要害机关和部门)大范围蔓延,这是中国计算机安全领域里的重大事件,它反映出我国计算机安全管理方面存在的问题。

5.计算机病毒的危害

任何计算机系统都有薄弱点,其操作系统也不可能尽善尽美。因此可以针对这些薄弱点设计各式各样的计算机病毒。就目前计算机病毒对计算机造成影响来看,主要包括对计算机网络的危害和对个人计算机的危害两个方面。

病毒对计算机网络的危害主要有下列几种:

⊙病毒程序通过"自我复制"传染正在运行的其它程序,与正常运行的程序争夺计算机资源。

⊙病毒程序可以冲毁存储器中的大量数据,致使计算机网络上其它用户的数据蒙受损失。

⊙病毒不仅侵害所使用的计算机系统,还侵害与该系统联网的其它计算机系统。

⊙病毒的程序可导致计算机控制的空中交通指挥系统失灵,银行金融系统瘫痪,卫星、导弹失控,工厂生产停滞,政府机构,事业部门秩序紊乱。

在我国,计算机网络还处于发展阶段,随着计算机的不断普及,我国计算机网络将迅速发展,可以肯定,在不久的将来计算机网络的安全会越来越重要。

病毒对个人计算机的危害主要有下列几种:

⊙破坏磁盘文件分配表,使用户在磁盘上的信息造成丢失。

⊙将非法数据写入 DOS 的内存参数区,引起系统崩溃。

⊙删除硬盘或软盘上特定的可执行文件或数据文件,修改或破坏数据文件。

⊙在磁盘上产生虚假坏簇,从而破坏有关的程序或数据文件。

⊙更改或重新写入磁盘的卷标号,对整个磁盘或磁盘上的特定磁道进行格式化。

⊙不断反复传染拷贝,造成存储空间减小,并影响系统运行效率。

⊙系统空挂,可以造成显示屏幕或键盘的封锁状态。

目前在我国,计算机病毒主要攻击的对象是个人计算机。

由上可知,一个小小的计算机病毒程序,可使一台微机、一个大型计算机系统或一个计算机网络处于瘫痪。这一方面反映了当今计算机系统的脆弱性,同时,另一方面也反映了计算机病毒已对计算机的安全构成了极大的威胁。

§1.4 计算机病毒在我国蔓延

计算机病毒在我国一出现,就以前所未有的速度迅速蔓延,是人们所料想不及的,下面我们分几个阶段来讨论。

1.计算机病毒的传入

我国大陆发现的第一个计算机病毒——小球病毒,就是由香港传入的。由于我国许多科学技术人员出国进修、考察,带回来一些计算机软件,特别是目前 INTERNET 网络在我国的发展,都为国外计算机病毒大量流入我国提供了方便。继小球病毒侵入我国以后,我国又出现了各种病毒不下 300 余种(不包括它们的变种)。截止到 1996 年底,据公安部计算机安全监察司不完全统计,全国约有 60% 的微机感染过计算机病毒,轻则影响工作正常进行,重则造成数据丢失,使许多单位造成严重的损失。

2.计算机病毒流传的原因

自从 1988 年 11 月的 INTERNET 网络事件后,五花八门的病毒便很快地在世界范围内相继登台亮相。为什么计算机病毒会呈现这样一种现象呢?其原因有以下几个方面:

(1)PC 机的普遍性

我们都知道,在人口密度越大的地方,瘟疫流行也越广、越快,其种类也越多。现在世界上各种计算机渗透到每个国家的政治、军事、经济及日常生活的各个方面。它们普及范围最广,涉及的领域最宽,因而也为病毒提供了流行、繁衍和变种的温床。

(2)网络的脆弱性

网络系统的各个组成部分、接口和界面、各层次的相互转换都存在着不少的漏洞和薄弱环节,尤其在软件方面。许多病毒因此得以在网络内广泛流行,如 IBM 圣诞树病毒、FU-SHOT4 病毒、UNIX 上的 Worm 病毒等。

(3)磁盘的脆弱性

计算机磁盘有三个最重要的部分:引导扇区(BOOT)、FAT 表、根目录区。引导扇区包含着计算机工作必需的指令及许多重要的信息。FAT 表是 DOS 以簇为单位用来给文件分配磁盘空间的,同一文件的所有簇在 FAT 表中链在一起。而文件目录区存放所有文件的目录。这三个部分是磁盘赖以正常使用的部分,又是十分脆弱的部分,自我防护性能差,很容易被替换、修改和破坏,因而早期病毒大都冲着这三个部分而来。

(4)DOS 系统的脆弱性

DOS 系统构成简单、系统开放。DOS 系统上的文件,为病毒提供了固定的攻击目标;同时 DOS 的可执行文件(.COM 或 .EXE 或批处理 .BAT 文件)的脆弱性也为病毒的攻击和传染大开方便之门;而文本文件、数据文件的任意可修改性更使病毒嵌入其中变得容易。

(5)硬件的脆弱性