IDG 系列资料—2

计算机病毒概论

An Introduction to Computer Viruses

国际数据集团
IDG 爱奇
INTERNATIONAL DATA GROUP
高技术公司研究部
IDG HIGH TECH—RESEARCH DEPT

计算机病毒概论

An Introduction to Computer Viruses

李向宇

国际数据集团
IDG 爱奇
INTERNATIONAL DATA GROUP
高技术公司研究部
IDG HIGH TECH—RESEARCH DEPT

序　言

计算机技术在飞速发展，计算机应用在不断普及，各种编程技巧在逐步提高，而计算机操作系统却存在着明显的弱点和漏洞，与此同时，计算机技术与计算机文化之间的发展又极不平衡，于是产生了当今攻击计算机系统的最可怕敌人——计算机病毒。

计算机病毒被喻为21世纪计算机犯罪的五大手段之一，并排序为第二。计算机病毒的攻击性，在于它能携带各种破坏程序并蔓延于应用领域。目前世界上几千万微机用户无时无刻不在受着计算机病毒的困扰，有些还陷入极度的恐慌。

但事实上，人们产生上述不安的原因，在于对计算机病毒的误解，所以有必要向广大计算机用户揭示计算机病毒的实质，使之对计算机病毒有个比较全面的认识和科学的态度。正是基于这种考虑，作者才编写了这一本书。

从1987年至今，计算机病毒已在世界上广泛蔓延开来，人们不断地对具体病毒进行剖析，研制开发了诊治、处理和免疫计算机病毒的各种软件。现在是否已经到了创建一门新兴学科——计算机病毒学的时候了。这是编写本书的第二个目的。

在编写过程中，作者力求集理论性和实用性于一体，既为想了解计算机病毒的广大科技工作者提供一本参考资料，又为正受计算机病毒困扰的广大用户提供一些实用方法。

由于编写时间十分仓促，编者水平有限，书中错误、遗漏以及不妥之处在所难免。恳请广大同行朋友给予批评指正。

在本书编写、出版过程中，得到了国际数据集团爱奇高技术公司研究部和北京地质局印刷厂激光照排车间的大力支持。在此，一并向他们致以谢意。

作者　李向宇

1990年4月5日于北京

目　录

第一章　计算机病毒的起源

继计算机的问世，计算机犯罪也随之出现，尤其到了计算机科学技术高速发展的八十年代末，在计算机安全领域中又出现了计算机病毒。计算机病毒对计算机系统安全性的威胁大大超过了以往各种计算机犯罪手段，而且，这种犯罪更具有高技术性。在本章中，我们将重点研究计算机病毒的起源。

第一节　计算机病毒产生的历史背景

随着计算机技术的迅速发展，计算机应用日趋深入和普及。计算机对人类发展的巨大贡献，使其在现代社会中居重要的战略地位。与此同时，计算机应用的社会化又带来了一系列新的问题，信息化社会面临着计算机病毒的严重威胁。计算机系统本身的脆弱性是计算机病毒产生的一个重要原因。

1.1　计算机系统本身的脆弱性

现代计算机系统的实现是安全性、开放性及制造成本的一种折衷，所以任何一种计算机系统都存在着脆弱性，即由折衷所带来的系统不安全的问题。这里，我们列举几个实例来说明计算机系统本身脆弱性的存在。

事实之一：1988 年联邦德国汉诺威大学计算机系一个 24 岁学生马蒂亚斯·斯佩尔，将自己的计算机系统同美国军方和军工承包商的 30 台计算机联网，在两年时间收集了大量有关美国国防情报的机密，其中包括美国"星球大战"计划，北美防空司令部、核武器和通信卫星等方面的情报。此举曾震惊了美国国防部和联邦调查局。另据报道，由于美国国家航空航天局在全世界的数据网保密系统存在着缺陷，联邦德国的一些计算机爱好者利用这些缺陷钻了空子。这些计算机爱好者通过打入"航天飞机"、"挑战者号"和"机密"等关键字，进入了美国航空航天局的数据网，便在屏幕上看到了有关"航天飞机 C 研究合同"、"系统的安全调查"和"助推火箭事故"等重要情报内容。这些计算机技术爱好者可以通过一些自己编制的程序接触美国国家航空航天局数据网用户的电子邮件，窃取信息，甚至可通过适当的程序设计手段使整个数据网络陷于瘫痪。

事实之二：1986 年 5 月，联邦德国的 4 名罪犯利用计算机系统通过适当手段改变信用卡的磁带密码，欺骗计算机系统，获得了 10 万马克，后经严密侦察，此案被破，4 名罪犯被捕。

事实之三：1986 年 12 月，法国银行发生了一起丢失几千万法郎的案件，这起利用计算机系统犯罪的案件，至今尚未侦破。

事实之四：1983 年，哥伦比亚发生了一起轰动一时的计算机盗窃案。1983 年 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 万美元过户到纽约大通银行

的一个户头上。次日，这笔款项从纽约大通银行过户到纽约的摩根信托保险银行，然后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，这笔巨款又转移到巴拿马的一家银行。由于一个同案犯没有正确文件提取现金，这笔巨款再一次转移到欧洲。此案在 1983 年 11 月暴露，警方经过 6 个月调查，有 12 个人被捕，主要案犯普利伊托（哥伦比亚发展部前秘书长）被警方拘捕，但由于缺乏证据，又被释放。事后，哥伦比亚中央银行的一位告密者在一起意外交通事故中丧生。

在我国，计算机犯罪也已出现，深圳、大连等地就出现过计算机犯罪案件。

在信息化社会，信息处理作为一个非常复杂的社会行为和现象，已经面临着来自各个方面的潜在威胁。

现实生活告诫人们，计算机系统所带来的信息处理高度自动化与高效化为人类的各项事务处理提供了极为有效的现代化手段，然而，计算机系统对于人类事物处理的潜在威胁类似核武器。这些威胁来自计算机系统故障、计算机犯罪，尤其是 80 年代末出现的计算机病毒。它关系到国家安全和防御，也关系到一个国家的政治、经济、科学技术等的正常活动。

西方国家的一位计算机专家根据已发生的案例多次提醒人们：一个国家的计算机应用同信息安全技术应当同时起步，即计算机文明与计算机技术的发展应同时起步，否则会造成严重后果和极大危害，这如同发展现代工业必须考虑环境保护和防止污染一样。

的确，计算机病毒的出现和迅速蔓延，在很大程度上反应了当今计算机系统的脆弱性，同时也反映了当今计算机应用的广泛性。计算机系统的各个组成部分、接口和界面、各个层次的相互转换，都存在着不少漏洞和薄弱环节。硬件设计缺乏整体安全性考虑。尤其是软件方面，一个系统的软件是由功能各不相同的程序模块构成的，是若干人年的劳动产物，开发者在思路上存在的差别使得这些软件易于存在隐患和潜在威胁。说到底，一个计算机系统（包括微型计算机系统）是在其软件运行过程中发现问题并不断改进和完善的。计算机系统对不同层次、不同界面上局部程序的改动，缺乏有效的测试手段，同时，人们对此也缺乏足够的敏感性。对计算机系统的测试，目前尚缺乏自动化的检测工具，更缺乏系统软件的完整检验手段。软件的手工生产方式，难以避免程序体系的大大小小修改和变动，这样，就使得计算机病毒很容易侵入系统。当今，计算机系统存在着以下问题：

(1) 缺乏整体安全性和完整性的设计和检测；

(2) 系统（包括硬件和软件）设计存在着局部合理与整体不合理的矛盾；

(3) 在软件不断完善和修改中，易于存在隐患和遭到病毒入侵的可能性。

(4) 任何一种软件都是由一定的计算机语言（汇编语言，PASCAL 语言、COBOL 语言、PL／I 语言以及 C 语言、C++语言等等）实现的，同种计算机语言在结构中的一致性可能导致非法模块链入合法程序之中，或非法程序取代合法程序的现象。

(5) 信息处理的完整性问题；

(6) 程序的互相调入问题；

(7) 安全性与方便性折衷的矛盾性问题。

任何一个计算机事件的发生都具有瞬时性、动态性和随机性。一个计算机犯罪事件通常可在 0.1ms−0.5ms 内发生，而且人们往往难于得到犯罪者留下的证据，这就极大地刺激了以计算机为工具的高技术犯罪案件的发生和发案率的迅速增加。

1.2 计算机犯罪的特点

(1) 计算机犯罪属于高技术犯罪，具有瞬时性和随机性，而且，人们也难于对犯罪者取证;

(2) 计算机犯罪是伴随现代化进程产生的，已成为当今世界发达国家和发展中国家面临的严重威胁和重大社会问题;

(3) 计算机病毒是计算机犯罪的一种新的衍化形式，它们对系统的破坏性亦是随编写者的目的而定的。它们可利用现有计算机犯罪手段，这种手段又比以往的计算机犯罪手段高明得多;

(4) 计算机系统的脆弱性是计算机病毒产生的基础，计算机系统的信息共享又是计算机病毒传播的首要条件;

(5) 计算机科学技术的发展，特别是微型计算机的普及、硬件和软件知识的透明度以及计算机使用方法的通用性等，是计算机病毒产生的实现环境和传播途径;

(6) 计算机病毒是一个国际性问题，真正要消除计算机病毒有待于国际间的合作。

实际上，计算机病毒的产生是计算机技术的高度发展与计算机文化尚未形成而出现的一种矛盾的结果。在计算机广泛普及应用的同时，计算机使用的各种管理方法及措施都不完善，各种计算机的使用者或爱好者有权编制任何程序并有机会在公共系统中运行，这是计算机病毒产生的一种原因。计算机技术是一种高科技，许多人或出于好奇心或出于某种别的目的也难免搞些恶作剧，这也是计算机病毒产生的一个根源。计算机系统不仅是一个可以使用的工具而且也是一种娱乐的工具，这是计算机病毒产生的另一种原因。

如果仔细追究病毒产生的根源，计算机信息资源共享途径没有得到很好的保护也是计算机病毒产生的一个原因。目前，网络系统的安全性还是一个急待研究的问题，口令加密的不安全性，在病毒发展的今天已经充分地体现出来。此外，软盘的随意使用和各种软件的非法拷贝，也是病毒产生的一个重要原因。

第二节　计算机病毒的起源说

计算机病毒的起源，到现在还没有一个为大家公认的确切说法。似乎所有计算专家、计算机用户都在不同程度上或不同立场上进行分析和判断，但现在还没有达到实质上的一致。尽管如此，似乎大家已有了一致的意见，这就是计算机病毒的发源地是美国。当然，计算机病毒发展到今天已不再是追溯计算机病毒起源的时候了，而是要认真对待这些已蔓延到整个世界计算机应用领域中的计算机病毒的时候了。

2.1 计算机病毒的种种起源说

关于计算机病毒的起源现在有几种说法：科学幻想起源说、恶作剧起源说、AT&T 公司游戏程序起源说、软件设计者软件自我保护起源说、美国软件俱乐部起源说以及美国中学生起源说等等。在这些起源说中还没有一个被人们所确认，也没有实质的论述予以证明。下面简单介绍一下这几种起源说。

(1) 科学幻想起源说

1977 年夏天，Thomas.J.Ryan 出版了一本幻想小说，该书全名叫《The Adolescence of p-1》。当时，这本书的作者幻想出了世界上第一个计算机病毒。这种病毒能从一个计算机到另一个计算机传染流行，能控制 7000 台计算机的操作系统。

当然，我们不否认这本书的问世对计算机病毒的产生及蔓延的作用。人类社会的许多现行科学技术，都是在先有幻想之后才成为现实的。也许在这本书问世之后，有些人才顿开茅塞，借助于他们对计算机硬件系统，尤其是对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。与此同时，1983 年美国计算机安全专家 Fred Cohen 通过实验证明了计算机病毒实现的现实性。至此，计算机病毒有了由幻想变成现实的理论依据。

(2) 恶作剧起源说

有资料介绍说，计算机病毒起源于搞恶作剧的人。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学校（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；而后者则大多是恶意的报复，想从受损失一方的痛苦中取得乐趣，以泄私愤。搞恶作剧的人一般并不是想在社会上广泛传染病毒，只是出于某种报复的目的（只限后者），一般不会是拿社会之广受损害而自娱。例如：在《计算机犯罪》一书中记录了这样一桩事实：某银行职员在计算机管理程序中插入了一小段程序，检查他的名字是否还在该银行系统的档案里，如果不在则破坏系统。结果，在他被炒了鱿鱼之后，该程序便对银行数据进行了破坏，从而达到了他个人的报复目的。

恶作剧者是信息社会高度发展的产物。他们对信息的读写或信息资源有着浓厚的兴趣。早在 1984 年，Steven Levy 所著的《Hackers》(《恶作剧者》) 一书就已向广大读者详细地介绍了恶作剧者的一切。正如 Levy 所说："恶作剧者是那些对某种（如计算机）技术感兴趣的人。他们似乎对所有的有关（如计算机）知识和技术均有兴趣，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。"

当然，恶作剧者也对给人类以自动化和信息处理高效率的计算机技术有着浓厚的兴趣，他们也完全可能对计算机系统的安全造成攻击。现在，关于计算机病毒的起源问题还没有定论，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。1988 年 11 月 3 日美国 Internet 网络蠕虫病毒的编写者 morris（莫里斯）实际上是一个计算机的恶作剧者，因为在他编写这个旨在渗透到美国国防部的计算机网络的病毒之时，也没有考虑到这种计算机病毒会给美国带来巨大的损失。直到走向法庭，他才对他所制造的这种病毒的具体影响有所了解。

这一实例说明，恶作剧者本身一般并没有很大的恶意，他们主要是要显示一下自己超群的计算机知识。

从实质上讲，计算机病毒的中学生起源说也应归结于恶作剧起源说，因为这些中学生编制计算机病毒的初衷亦不是恶意的。有关资料显示，计算机犯罪大多为一些年轻人。他们自恃自己高超的计算机技术以及对计算机操作系统的深入了解，编制了破坏计算机系统的程序。在已发现的计算机犯罪案件中，犯罪者的年龄都在 18 至 46 岁之间，平均为 25 岁左右。目前，随着计算机应用的普及，尤其是在美国，计算机家庭占有率较高。许多年轻的大学生和中学生很容易接触计算机，他们对计算机语言和操作系统（尤其是 IBM PC AT、

XT 机使用的 MS-DOS 及 PC-DOS）都有相当的了解。有资料说，计算机病毒是美国一些十几岁到二十来岁的计算机爱好者想出来的。这些被人们认为是计算机"神童"的娃娃一开始只是想编写一些程序和自己的伙伴开个玩笑，一要显示一下自己的知识实力，二要从朋友的机器资源损失中求得乐趣。然而，这种玩笑开得越来越大，范围也越来越广。这些搞恶作剧的年轻人，把恶作剧的程序存储在软磁盘上（其中大部分为游戏盘）同不知情的人交换软盘，从而引起了计算机病毒的广泛传染及蔓延。后来，效妨者日众，病毒的种类日增，制造病毒的目的也开始起了变化，计算机病毒由点到面以至扩展到了整个社会，最后成了计算机安全领域中的大问题。

(3) AT&T 公司游戏程序起源说

关于计算机病毒起源的另一种猜想是，在十几年前，当计算机刚刚在社会上得到应用和逐渐普及的时候，美国贝尔实验室计算机人员，为了娱乐，而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。有人认为这是第一个计算机病毒。但是，持这种看法的人为数不多，因为从历史延续的角度来讲，计算机病毒是近几年才出现的事情，甚至到现在，尽管计算机病毒是众所周知的，但在理论上和认识上，人们并不十分清楚，许多人还不真正地了解这一"新生事物"。

贝尔实验室的游戏程序的确带有一定的破坏性。那么，这种破坏性程序是否具有传染性呢？也许当时由于计算机还没有普及应用，所以病毒没有传染开来。但实际上，只要病毒出现，它就会导致传染。从十几年前到病毒出现的近年间只一个病毒"冷冻"时期。所以作为一种起源的学说，它没有历史的延续性。再者，如果当时的游戏程序具有广泛的传染性，那么对下一个具有传染性的程序的设计技术应该有人能够预见到，但事实却相反。

所以我们若把病毒的出现归罪于 AT&T，似乎有些不太合乎情理。这种看法或观点，也许只是少数人的一种观点。

当然，偶然的事情也会存在。当时"冷冻"起来的并不认为是"病毒"的那种程序设计技术，在后来的病毒开发中也许起了指导作用。所以，从这一方面来讲，作为一种起源说也不是没有一点道理的。

(4) 软件制造商软件保护起源说

计算机软件是一种知识密集的高科技产品，计算机软件技术发展到一定程度，人们对于软件资源的保护并不尽合理。这样使得许多合法软件的非法复制或拷贝的现象极为平常，从而使得软件制造商的利益受到了严重的侵害。于是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最终结果。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。也正因为如此，许多人大肆宣传合法软件的使用的好处。但事实上，只要病毒存在，无论合法软件还是非法软件都要受到计算机病毒的侵害。所以把病毒的产生归罪于软件保护的说法，确实有些牵强。不过对 Pakistani Brain 病毒的说法，在一定程度上又是对软件保护起源说的一种证实。即有人认为，Brain 是巴基斯坦两兄弟为了追踪非法复制其软件产品的用户而编制的，它最初的"毒性"并不大，只是修改卷标，把卷标改为（C）Brain，但这也并不能说明软件自我保护是病毒产生的唯一途径。

(5) 美国软件俱乐部计算机病毒起源说

美国计算机软件使用者俱乐部是由那些志同道合的计算机技术爱好者组成的一个团体。这些计算机爱好者通过这一组织，利用计算机网络分享彼此的设计心得。也有的人在公告板上显示自己发明的程序并注明欢迎大家通过网络来选用，但在一定时间内必须邮寄使用费用。通常这种公告板上的程序"暗藏杀机"，如果有人使用了这项程序却不付费用的话，在特定的时间内，暗藏在程序中的计算机病毒就像定时炸弹一样开始爆发，藉以警告那些"占便宜"的使用者。如果使用者乖乖地寄上费用的话，设计者会寄上解毒程序。如果不知内情的"盗用者"把这种带着病毒的程序分享给其他朋友或亲友，于是一传十，十传百，计算机病毒就广泛传染开来。这样，美国的软件俱乐部就成了计算机病毒的起源，他们无心插柳柳成荫，而成了电子计算机病毒的摧生者。这种说法似乎还很有道理。

2.2 难以考证的事实

计算机病毒的罪魁祸首倒底是谁？到目前为止，依然众说纷纭。有人说 1984 年，美国计算机专家 FredCohen 在美国国家计算机安全会议上演示过病毒的实验（他对计算机病毒的研究始于 1983 年），所以世界上第一个计算机病毒是由他创造的。但实际上，计算机病毒的广泛传染始于 1987 年，1988 年开始得到人们的重视，尤其是 1988 年 11 月 3 日以后一直到现在，计算机病毒几乎为计算机界人士所周知。计算机病毒起源的这一复杂的历史问题是很难考证的。

但是可以相信，计算机病毒的产生并广泛传染至全世界的根本原因在于那些对于计算机语言及操作系统有深入了解的一些恶作剧者。不过，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，而且有些计算机病毒创造者的本意也并非是要损害计算机系统。

无论如何，计算机病毒已在社会上广泛传播，世界上许多个人计算机及计算机网络都受到了病毒的攻击。现在摆在我们每一个计算机安全人员面前的问题是怎样预防和消除病毒，而不是探讨计算机病毒的起源问题；我们的任务是如何清除病毒给社会带来的恶果，而不是去追踪它的历史。

总之，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。

第三节　本章小结

现在，计算机病毒已经成了广大计算机用户普遍熟知的一种威胁计算机安全的最重要的手段。它是比任何计算机犯罪手段都高明的手段，在当今计算机技术不断发展的同时，计算机病毒技术也在不断发展，计算机病毒种类及其传染用户的不断增多使得它已经成为一个广泛的社会问题，即：计算机病毒正在社会上广泛蔓延开来。

第二章　计算机病毒的蔓延与现状

时至今日，计算机病毒已经出现在我们周围，但我们却很难判定计算机病毒的真正起源，人们只是猜测计算机病毒产生的可能根源，并无时无刻不在关心着出现在计算机安全领域中的最大的敌人——计算机病毒将会给人类的信息化社会带来多大的灾难。计算机病毒究竟能够传染多大的范围，这种传染能否得到控制或局部的限制。这也是计算机安全专家、系统管理员以及计算机用户所关心的问题。的确，事实已经说明计算机病毒的出现给人类社会的物质财富带来了极大的损失，并严重地影响着计算机系统的普及应用，甚至影响着计算机技术的高速发展。

第一节　Internet 网络事件的风波

1988 年 11 月 3 日，美国最大的计算机网络 Internet 网络遭到了计算机病毒的攻击，从此，在国际计算机领域掀起了一个谈论病毒的高潮。

1.1　Internet 网络事件

Internet 网络是使用 Unix 为主要操作系统的网络。1988 年 11 月 2 日，该网络受到计算机病毒的严重攻击，Internet 网络中的约 6200 台基于 Unix 的 VAX 系列小型机及 Sun 工作站都染上了病毒，计算机用户的损失约 9200 多万美元。Internet 网络中出现的病毒是一种蠕虫程序，它利用 Unix 系统中电子邮件的一种脆弱性而进入 Internet 网络，并在网络中不断自我复制，1988 年 11 月 2 日至 11 月 3 日一夜之间为计算机用户造成了巨大损失。这一事件极大地震惊了 AT&T 公司。从此，Unix 系统的安全性问题提到了计算机科学工作者的研究日程。

许多资料介绍说，Internet 网络病毒是一个卡内尔（cornell）大学计算机专业毕业的、当时年仅二十三岁的 Robert T.Morris Jr.编写的，它编写这一程序的用意是把无害的“病毒”慢慢地渗透到政府及研究机构的计算机网络系统中，其行为是一种恶作剧的行为，但当他将这一程序置入计算机网络系统之后，这一程序以闪电般的速度不断地复制自己，并向整个网络迅速蔓延开来，网络系统因“病毒”的侵害而遭到堵塞和瘫痪。

实际上，就 Morris 编写的蠕虫程序实质而言，这一病毒程序主要是利用了 Berkeley 大学的 Unix 4.3 版本的一个漏洞。根据后来 Unix 专家的分析，Morris 的病毒程序以三种途径侵入 Internet 网络系统：

（1）利用 Berkeley Unix 4.3 版“Sendmail”中的一个程序漏洞使调试位呈通态；

（2）在“finger”程序的一部分中使缓冲器过载，使之对病毒程序的另一部分进行编译和链接；

（3）获取口令，进入网络。

这样，当病毒进入 Internet 之后，通过自我复制，攻击 Sun 的工作站及 DEC 的 VAX 系列小型机。为此，美国国防部在卡内基—梅隆大学的软件工程学院设立了一个由 100 名计算机专家组成的专门队伍，以研究国防部门计算机系统对计算机病毒的防范问题以及及时了解并监视 Internet 网络的安全情况，以便了解病毒对 Internet 网络的攻击情况。

1.2 Internet 网络事件的制造者

有资料介绍，Morris 是美国政府高级计算机专家的儿子，早在上中学时，他的癖好就转向了计算机。起初，Morris 只是在家里用计算机做一做学校作业。但不久后，他掌握了复杂的数学计算方法及计算机编程技术，从而开始编写计算机程序，并对计算机系统（尤其是操作系统）有了较深的了解。Morris 17 岁时到贝尔实验室工作。后来他参加了哈佛大学计算机计划，在该大学心理学计算中心当程序员。从此，对计算机系统更有了进一步的了解。在此之后他进入了 Cornell 大学的计算机系，开始了对计算机系统的系统学习及研究。

Morris 编写的攻击 Internet 网络的病毒程序已经成了事实。Morris 本人也已在 1989 年 7 月被推上了美国地方法庭。

1.3 Internet 网络事件的余波

现在，Internet 网络受到病毒攻击这一事实已经成了过去，侵入网络中的病毒已被清除，网络也恢复了正常运转。但人们不难想到：①Unix 作为一个多用户的且开放性好的操作系统，其安全性如何呢？②在世界高技术发达的国家现已有了许多计算机网络，那么网络的安全性又如何处理呢？③病毒已经出现，面对将来的发展，又怎样对付这令人头痛的病毒？④病毒的设计者，可能是有意的也可能是无意的，可能是恶意的，也可能是无恶意的，但最终结果已造成了社会财富的巨大的损失，那么病毒的制造者应承担什么责任呢？计算机病毒已经能够攻击小型机及微机，那么大型机是否也会遭到攻击呢？……这些问题，都是摆在我们面前的难题。因为计算机系统及网络本身就是开放性与安全性的一种折衷，侧重于哪一方面都会导致另一方面的削弱。

Internet 网络的病毒是攻击 Sun 工作站及 DEC VAX 小型机的，而对于其他与之不兼容的系统则没有攻击性，这也从一个侧面反映了病毒破坏的针对性。尽管在病毒出现之后，11 月 18 日成立的 CERT 负责对 Internet 网络系统提供了较好的安全服务，但用户对 Unix 系统的安全问题仍然顾虑重重，AT&T 也受到了震惊，甚至有些用户指责 Sun 及 DEC。到目前为止，Unix 的一些漏洞仍未得到完善。Internet 受攻击的可能仍然存在。现在已形成了这样一种局面：对计算机网络的安全性问题，要么寻求一条建立网络的新途径，要么牺牲方便性和开放性以求得安全性。

第二节　计算机病毒在国外的蔓延与现状

据有关资料介绍，在 1987 年到 1989 年间已出现的各种计算机病毒不下 80 余种。更有甚者宣称，计算机病毒种类有 156 种之多。这些统计数据虽差别很大，但它从一个侧面反映了计算机病毒的传染和蔓延范围，同时也反映了计算机病毒对计算机系统资源威胁的严重性。自 1988 年 11 月至今，计算机病毒在短短两三年间就传遍了世界，引起了世界范围的恐

慌和警觉。

80年代以来，IBM PC及其兼容机得到了极大的普及。到目前为止，世界共安装这一类系统总计2300多万台，成为各种类型机器中装机量最多的一种，因此，它也就成了计算机病毒攻击的主要对象。

(1) 攻击 *IBM PC* 及其兼容机的病毒

据统计，世界上目前已发现的计算机病毒约80多种，其中攻击IBM PC及其兼容机的达44种之多。这44种计算机病毒是：

New Jerusalem;
Yankee Doodle;
Ashar;
Disk Killer / Ogre;
Mix I;
3551 / Syslock;
Ohio;
Swap / Israeli Boot;
Icelandic;
405;
FuManchu / 2086;
1701 / CasCade;
Stoned / Marijuana;
1704 / CasCade / Falling;
Letter;
Ping Pong-B / Falling Letter Boot;
Den Zuk;
Ping Pong / Italian / Bouncing Dot /
Bouncing ball;
Vienna-B;
Vienna / 648 / DOS-68;
Yale / Alameda;
Jerusalem / 1813;
Survivo2;
Pakistani Brain / Brain;
Alabama;
2930;
Aids / VGA2CGA;
1536 / Zero Bug;
Dark Avenger;
Vacsina;
TyPO;