高等教育质量工程信息技术系列示范教材

信息系统安全教程（第2版）

张基温 编著

清华大学出版社

高等教育质量工程信息技术系列示范教材

信息系统安全教程
(第2版)

张基温 编著

清华大学出版社
北京

内 容 简 介

本书从应用的角度介绍计算机信息系统安全技术。全书按照“威胁—防护—管理”的思路组织为5章，内容包括信息系统威胁、数据安全保护、身份认证与访问控制、网络安全保护和信息系统安全管理。

本书深入浅出，结构新颖，紧扣本质，适合教学，可以激发学习者的热情。书中还配有丰富的实验和习题，供学习者验证和自测。本书适合作为计算机科学与技术专业、信息管理与信息系统专业、网络专业和信息安全专业的“信息系统安全概论”课程的教材或教学参考书，也可供有关技术人员参考。

图书在版编目(CIP)数据

信息系统安全教程/张基温编著．--2版．--北京：清华大学出版社，2015
高等教育质量工程信息技术系列示范教材
ISBN 978-7-302-37241-7

Ⅰ．①信…　Ⅱ．①张…　Ⅲ．①信息系统－安全技术－高等学校－教材　Ⅳ．①TP309

中国版本图书馆CIP数据核字(2014)第153430号

责任编辑：白立军　战晓雷
封面设计：常雪影
责任校对：时翠兰
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮 购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：19.75　　**字　　数**：483千字
版　　次：2007年8月第1版　2015年1月第2版　　**印　　次**：2015年1月第1次印刷
印　　数：1～2000
定　　价：34.50元

产品编号：058871-01

前　言

（一）

信息系统是重要的，重要的系统需要特别保护；计算机信息系统是复杂的，复杂的系统是脆弱的，脆弱的系统也需要特别保护；计算机信息系统是虚拟的，虚拟的系统给安全保护带来很大困难；现代信息系统是开放的，开放的系统会带来更多的风险。重要、复杂、虚拟和开放，也给人们带来研究的乐趣和商业机会。现在信息系统安全技术和产品已经大量涌现，并且还在不断发展。

本书的目的是介绍计算机信息系统安全原理。作为一本原理类的教材，关键的问题是要梳理成合理而又容易理解和掌握的体系。在教学实践中，笔者反复探索，将安全理论梳理成如下 3 大类：

（1）攻防技术。恶意程序、网络攻击（黑客）、隔离（逻辑隔离——防火墙、物理隔离和电磁防护）、安全监控（IDS、网络诱骗和审计）、紧急响应和取证。

（2）安全信任体系。加密与信息隐藏、认证、安全协议。

（3）安全体系结构和评估标准。

这样的梳理基本上囊括了几乎所有的安全技术，并且较为本质。

在内容的安排上，考虑了如下原则：

（1）尽量把与其他技术或概念相关的内容排在后面，即与其他内容相关最少的排在最前面。

（2）将能引起兴趣的内容排在前面，以使学习者能有成就感。

（3）把安全体系结构和安全等级放在最后，这样不仅使其内容容易理解，而且也是对前面内容的总结和提高。

在内容的取舍上采取的原则是：重点内容详细介绍，次要内容只做一般介绍。

本书每章最后都配备了较多的习题。这些习题有不同的类型：

- 有些要思考、总结；
- 有些要进一步理解；
- 有些要自己想象；
- 有些要查找资料；
- 有些要动手实验。

本书的第 1 版正是基于这些考虑而形成的。

（二）

常言道："道高一尺，魔高一丈"。信息系统安全是针对入侵和攻击采取的一系列安全策略和技术。然而，按照木桶原理，当一块短的木板被加长后，另一块次短的木板就变成最

短的木板了；而一种攻击被防御之后，新的攻击又会出现。在这个充满竞争的世界里，攻击与防御相伴而生并且永不会完结，攻与防的博弈将在竞争中永无止境。一般说来，防御往往要比攻击付出更多的代价，这是因为

- 攻击可以择机发起，防御必须随时警惕。
- 攻击可以选择一个薄弱点实施，防御必须全线设防。
- 攻击一般使用一种或几种技术，防御则需要考虑已知的所有技术。
- 攻击可以肆意进行，防御必须遵循一定的规则。

社会总在发展，技术总在进步，攻击与防御也在博弈中相互促进。信息系统安全作为一门新兴的技术和学科，在本书第1版出版后的近7年间，又有了长足的发展。在读者和出版社的不断呼吁下，笔者下大力气进行全面修订。

教材不是一般科技书，在编写过程中首先要考虑如何教的问题。为了更适应教学，第2版按照“威胁(第1章)—防护(第2～4章)—管理(第5章)”的体系进行组织。这相当于“提出问题—解决问题—总结提高”的思路。经过本人一个学期的试讲，效果不错。

同时，本书还在内容上进行了删增。删除了已经不再使用的技术，如DES加密算法等；增添了新技术的内容，如AES密码、流密码、僵尸网络等。

对信息系统的攻击种类繁多，形式多样，但概括起来不外乎两个方面：非法窃取和使系统异常。

(三)

虽然本人认为第2版比第1版有了不少改进，但个人能力和客观条件有限，加之社会还在发展，技术还在进步，在这个新的社会重要领域中还会出现许多新的问题和解决方案，因此修订应当是一个长期的工作。在本书第2版即将出版之际，衷心地希望读者和有关专家能不吝指正，以便适当的时候再进一步修订。

在本书(包括第1版)的编写过程中，得到赵忠孝(福州外语外贸学院)以及张秋菊、董兆军、张展为、张友明、史林娟、张展赫、戴璐、刘诗瑾、廖伟国以及我的研究生陶利民、蒋中云、王玉斐、魏士婧、董瑜的不少帮助，在此谨向他们表示感谢。

本书在编写过程中还参考了大量资料。这些资料有的引自国内外论文，有的引自其他著作，有的引自网站。虽本人尽心在参考文献中予以列出，但仍会有许多疏漏，同时也受篇幅所限，未能将所有参考资料一一列出。在此谨向有关作者致谢。

张基温

2014年8月

目　录

第1章 信息系统安全威胁

信息系统安全威胁(thread)是指对于信息系统的组成要素及其功能造成某种损害的潜在可能。信息系统是现代社会中的重要系统,重要系统往往正是攻击者的首选目标;信息系统也是一个复杂的系统,复杂系统所具有的神秘性往往会刺激好奇者、好胜者和恶作剧者的攻击兴趣,并且其本身也有过多的脆弱。

攻击可能以获取系统中的信息为目的——信息窃取型攻击,也可能使系统无法正常运行——系统破坏型攻击,还可能控制系统,让系统成为其帮凶。

从形式上看,攻击大致有如下3种:

(1) 恶意代码攻击,包括病毒、特洛伊木马、蠕虫、细菌、陷门和逻辑炸弹等。

(2) 窃听攻击,包括声波窃听、电磁波窃听、光缆监听、手机窃听和网络窃听。

(3) 黑客攻击,包括消息采集攻击、代码漏洞攻击、欺骗和会话劫持攻击、分布式攻击等。

本章介绍这些攻击的各种具体表现。

1.1 计算机病毒

在生物学界,病毒(virus)是一类没有细胞结构,但有遗传、复制等生命特征,主要由核酸和蛋白质组成的有机体。计算机病毒(computer virus)是有与生物界中的病毒极为相似特征的程序。在《中华人民共和国计算机信息系统安全保护条例》中,病毒代码被明确定义为"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"。

通常,人们也简单地把计算机病毒定义为:利用计算机软件与硬件的缺陷,破坏计算机数据并影响计算机正常工作的一组指令集或程序代码。更广义地说,凡是能够引起计算机故障,破坏计算机数据的程序代码都可称为计算机病毒。

1.1.1 病毒的特征

1. 传染性

传染是病毒最本质的特征之一,是病毒的再生机制。生物界的病毒可以从一个生物体传播到另一个生物体,病毒也可以从一个程序、部件或系统传播到另一个程序、部件或系统。在单机环境下,病毒的传染基本途径是通过磁盘引导扇区、操作系统文件或应用文件进行传染;在网络中,病毒主要是通过电子邮件、Web页面等特殊文件和数据共享方式进行传染。

一般将传染分为被动传染和主动传染。通过网络传播或文件复制,使病毒由一个载体被携带到另一个载体,称为被动传染。病毒处于激活状态下,满足传染条件时,病毒从一个

载体自我复制到另一个载体，称为主动传染。

从传染的时间性上看，传染分为立即传染和伺机传染。病毒代码在被执行瞬间，抢在宿主程序执行前感染其他程序，称为立即传染。病毒代码驻留内存后，当满足传染条件时才感染其他程序，称为伺机传染。

2. 潜伏性与隐蔽性

病毒一旦取得系统控制权，可以在极短的时间内传染大量程序。但是，被感染的程序并不是立即表现出异常，而是潜伏下来，等待时机。

病毒的潜伏性还依赖于其隐蔽性。为了隐蔽，病毒通常非常短小，一般只有几百字节或上千字节，此外还寄生于正常的程序或磁盘较隐蔽的地方，也有个别以隐含文件形式存在，不经过代码分析很难被发觉。

3. 寄生性

寄生是病毒的重要特征。病毒实际上是一种特殊的程序，必然要存储在磁盘上，但是病毒为了进行自身的主动传播，必须使自身寄生在可以获取执行权的寄生对象——宿主程序上。

就目前出现的各种病毒来看，其寄生对象有两种，一种是寄生在磁盘引导扇区；另一种是寄生在可执行文件(.EXE 或.COM)中。这是由于不论是磁盘引导扇区还是可执行文件，它们都有获取执行权的可能，这样病毒寄生在它们的上面，就可以在一定条件下获得执行权，从而使病毒得以进入计算机系统，并处于激活状态，然后进行病毒的动态传播和破坏活动。对于寄生在磁盘引导扇区的病毒来说，病毒引导程序占有了原系统引导程序的位置，并把原系统引导程序搬移到一个特定的地方。这样系统一启动，病毒引导模块就会自动地装入内存并获得执行权，然后该引导程序负责将病毒代码的传染模块和发作模块装入内存的适当位置，并采取常驻内存技术以保证这两个模块不会被覆盖，接着对该两个模块设定某种激活方式，使之在适当的时候获得执行权。处理完这些工作后，病毒引导模块将系统引导模块装入内存，使系统在带毒状态下运行。对于寄生在可执行文件中的病毒来说，病毒一般通过修改原有可执行文件，使该文件一执行就先转入病毒引导模块。该引导模块也完成把病毒的其他两个模块驻留内存及初始化的工作，然后把执行权交给执行文件，使系统及执行文件在带毒的状态下运行。

病毒的寄生方式有两种，一种是替代法；另一种是链接法，所谓替代法是指病毒用自己的部分或全部指令代码替代磁盘引导扇区或文件中的全部或部分内容。所谓链接法则是指病毒将自身代码作为正常程序的一部分与原有正常程序链接在一起，病毒链接的位置可能在正常程序的首部、尾部或中间，寄生在磁盘引导扇区的病毒一般采取替代法，而寄生在可执行文件中的病毒一般采用链接法。

4. 非授权执行性

一个正常的程序是由用户调用的。被调用时，要从系统获得控制权，得到系统分配的相应资源，来实现用户要求的任务的。病毒虽然具有正常程序所具有的一切特性，但是其执行

是非授权进行的：它隐蔽在合法程序和数据中，当用户运行正常程序时，病毒伺机取得系统的控制权，先于正常程序执行，并对用户呈透明状态。

5. 可触发性

潜伏下来的病毒一般要在一定的条件下才被激活，发起攻击。病毒具有判断这个条件的功能。下面列举一些病毒的触发(激活)条件。

(1) 日期/时间触发：病毒读取系统时钟，判断是否激活。例如，“黑色星期五”逢 13 日的星期五发作等，CIH-1.2 版于每年的 4 月 26 日发作，CIH-1.3 则在 6 月 26 日发作，CIH-1.4 的发作日期则为每个月的 26 日。

(2) 计数器触发：病毒内部设定一个计数单元，对系统事件进行计数，判定是否激活。例如，2708 病毒当系统启动次数达到 32 次时被激活，发起对串、并口地址的攻击。

(3) 键触发：当输入某些字符时触发(如 AIDS 病毒，在输入 A、I、D、S 时发作)、或以击键次数(如 Devil's Dance 病毒在用户第 2000 次击键时被触发)或按键组合等为激发条件(如 Invader 病毒在按下 Ctrl+Alt+Del 键时发作)。

(4) 启动触发：以系统的启动次数作为触发条件。例如，Anti-Tei 和 Telecom 病毒当系统第 400 次启动时被激活。

(5) 感染触发：以感染文件个数、感染序列、感染磁盘数或感染失败数作为触发条件。例如，Black Monday 病毒在运行第 240 个染毒程序时被激活；VHP2 病毒每感染 8 个文件就会触发系统热启动操作等。

(6) 条件触发：用多种条件综合使用，作为病毒代码的触发条件。

6. 破坏性

破坏性体现了病毒的杀伤能力。大多数病毒还具有破坏性，并且其破坏方式总在花样翻新。常见的病毒破坏性有以下几个方面：

(1) 占用或消耗 CPU 资源以及内存空间，导致一些大型程序运行受阻，系统性能下降。

(2) 干扰系统运行，例如不执行命令、干扰内部命令的执行、虚发报警信息、打不开文件、内部栈溢出、占用特殊数据区、时钟倒转、重启动、死机、文件无法存盘、文件存盘时丢失字节、内存减小、格式化硬盘等。

(3) 攻击 CMOS。CMOS 是保存系统参数(如系统时钟、磁盘类型、内存容量等)的重要场所。有的病毒(如 CIH 病毒)可以通过改写 CMOS 参数破坏系统硬件的运行。

(4) 攻击系统数据区。硬盘的主引导记录、分区引导扇区、FAT(文件分配表)、文件目录等是系统重要的数据，这些数据一旦受损，将造成相关文件的破坏。

(5) 攻击文件。现在发现的病毒中，大多数是文件型病毒。这些病毒会使染毒文件的长度、文件存盘时间和日期发生变化。

(6) 干扰外部设备运行，如封锁键盘、产生换字、抹掉缓存区字符、输入紊乱、使屏幕显示混乱以及干扰声响、干扰打印机等。

(7) 破坏网络系统的正常运行，例如发送垃圾邮件、占用带宽，使网络拒绝服务等。

1.1.2 病毒的分类

按照不同的分类标准，病毒可以分为不同的类型，下面介绍几种常用的分类方法。

1. 按照所攻击的操作系统分类

- DOS 病毒：攻击 DOS 系统。
- UNIX/Linux 病毒：攻击 UNIX 或 Linux 系统。
- Windows 病毒：攻击 Windows 系统，如 CIH 病毒。
- OS/2 病毒：攻击 OS/2 系统。
- Macintosh 病毒：攻击 Macintosh 系统，如 Mac. simpsons 病毒。
- 手机病毒。
- 网络病毒。

2. 按照寄生位置分类

1）引导型病毒

引导型病毒是寄生在磁盘引导区的病毒。图 1.1 显示了硬盘的逻辑结构。可以看出，磁盘有两种引导区：主引导区和分区的引导区。所以也就有两种引导型病毒：

（1）MBR 病毒，也称主引导区病毒。该类病毒寄生在硬盘主引导程序所占据的硬盘 0 头 0 柱面第 1 个扇区中，典型的病毒有大麻病毒、2708 病毒、火炬病毒等。

（2）BR 病毒，也称为分区引导病毒。该类病毒寄生在硬盘活动分区的逻辑 0 扇区（即 0 面 0 道第 1 个扇区），典型的病毒有 Brain、小球病毒、Girl 病毒等。

2）文件型病毒

按照所寄生的文件类型可以分为 4 类：

（1）可执行文件，即扩展名为 COM、EXE、PE、BAT、SYS、OVL 等的文件。一旦运行这类病毒的载体程序，就会将病毒注入、安装并驻留在内存中，伺机进行感染。感染了该类病毒的程序往往会减慢执行速度，甚至无法执行。

（2）文档文件或数据文件，例如 Word 文档、Excel 文档、Access 数据库文件。宏病毒（Macro）就感染这些文件。

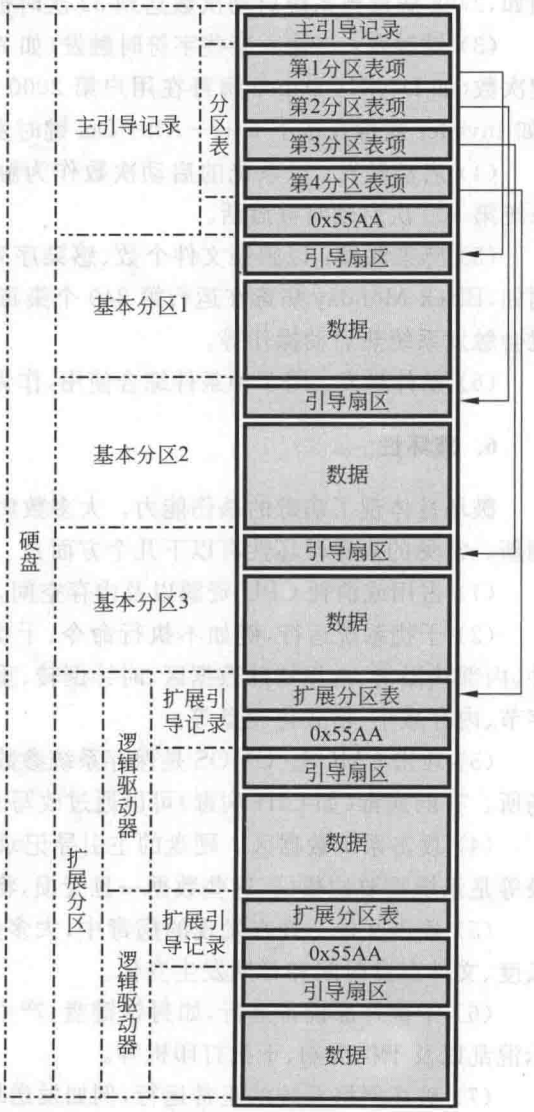

图 1.1　磁盘逻辑结构

(3) Web 文档，如 HTML 文档和 HTM 文档。已经发现的 Web 病毒有 HTML/Prepend 和 HTML/Redirect 等。

(4) 目录文件，如 DIR2 病毒。

3) 引导兼文件型病毒

这类病毒在文件感染时还伺机感染引导区，例如 CANCER 病毒、HAMMER Ⅴ病毒等。

4) CMOS 病毒

CMOS 是保存系统参数和配置的重要地方，它也存在一些没有使用的空间。CMOS 病毒就隐藏在这一空间中，从而可以躲避磁盘的格式化清除。

3. 按照是否驻留内存分类

1) 非驻留(nonresident)病毒

非驻留病毒选择磁盘上一个或多个文件，不等它们装入内存，就直接进行感染。

2) 驻留(resident)病毒

驻留病毒装入内存后，发现另一个系统运行的程序文件后进行传染。驻留病毒又可进一步分为以下几种：

(1) 高端驻留型。

(2) 常规驻留型。

(3) 内存控制链驻留型。

(4) 设备程序补丁驻留型。

4. 按照病毒形态分类

(1) 多态病毒。这种病毒形态多样。它们在复制之前会不断改变形态以及自己的特征码，以躲避检测。例如，最臭名昭著的“红色代码”病毒几乎每天变换一种形态。

(2) 隐身病毒。隐身病毒对所隐身之处进行修改，以便藏身。分为两种情形：

- 规模修改：病毒隐藏感染一个程序之后，立即修改程序的规模。
- 读修改：病毒可以截获已感染引导区记录或文件的读请求并进行修改，以便隐藏。

(3) 逆录病毒。这是一种攻击病毒查防软件的病毒。分为 3 种攻击方式：

- 关闭病毒查防软件。
- 绕过病毒查防软件。
- 破坏完整性校验软件中的完整性数据库。

(4) 外壳病毒。这种病毒为自己添加一层保护外套，躲过病毒查防软件的检测、跟踪和拆卸。

(5) 伴随病毒。这种病毒首先创建可执行文件，并在此基础上扩展，以便抢先执行。

(6) 噬菌体病毒。这种病毒用自己的代码替代可执行代码，可以破坏接触到的任何可执行程序。

5. 按照感染方式分类

按照感染方式，文件型病毒可以分为如图 1.2 所示的几种类型。

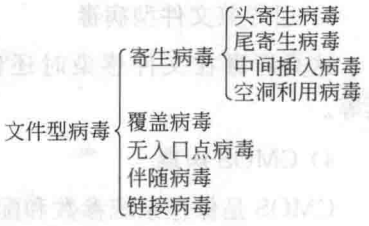

图 1.2　文件型病毒分类

(1) 寄生病毒。这类病毒在感染的时候，将病毒代码加入正常程序之中，原来程序的功能部分或者全部被保留。根据病毒代码加入的方式不同，寄生病毒可以分为头寄生、尾寄生、中间插入和空洞利用 4 种。

头寄生是将病毒代码加入文件的头部。具体有两种方法：一种是将原来程序的前面一部分复制到程序的最后，然后将文件头用病毒代码覆盖；另外一种是生成一个新的文件，首先在头的位置写上病毒代码，然后将原来的可执行文件放在病毒代码的后面，再用新的文件替换原来的文件，从而完成感染。头寄生方式适合于不需要重新定位的文件，如批处理病毒和 COM 文件。

尾寄生是将病毒代码加入文件的尾部，避开了文件重定位的问题，但为了先于宿主文件执行，需要修改文件头，使用跳转指令使病毒代码先执行。不过，修改头部也是一项复杂的工作。

中间插入是病毒将自己插入被感染的程序中，可以整段插入，也可以分成很多段，靠跳转指令连接。有的病毒通过压缩原来的代码的方法保持被感染文件的大小不变。

空洞利用多用于视窗环境下的可执行文件。因为视窗程序的结构非常复杂，其中都会有很多没有使用的部分，一般是空的段或者每个段的最后部分。病毒寻找这些没有使用的部分，然后将病毒代码分散到其中，这样就实现了难以察觉的感染(著名的 CIH 病毒就使用了这种方法)。

(2) 覆盖病毒。这种病毒的手法极其简单，是初期的病毒感染技术，它仅仅直接用病毒代码替换被感染程序，使被感染的文件头变成病毒代码的文件头，不用作任何调整。

(3) 无入口点病毒。这种病毒并不是真正没有入口点，在被感染程序执行的时候，并不立刻跳转到病毒的代码处开始执行，病毒代码无声无息地潜伏在被感染的程序中，可能在非常偶然的条件下才会被触发，开始执行。采用这种方式感染的病毒非常隐蔽，杀毒软件很难发现在程序的某个随机的部位有这样一些在程序运行过程中会被执行到的病毒代码。

大量的可执行文件是使用 C 语言编写的，这些程序有这样一个特点，程序中会使用一些基本的库函数，比如字符串处理、基本的输入输出等。为了使用这些库函数，编译器会在启动用户开发的程序之前增加一些代码对库进行初始化。这给了病毒一个机会，病毒可以寻找特定的初始化代码，并修改这段代码的开始语句，使得执行完病毒之后再执行通常的初始化工作。“纽克瑞希尔”病毒就采用了这种方法进行感染。

(4) 伴随病毒。这种病毒不改变被感染的文件，而是为被感染的文件创建一个伴随文件(病毒文件)，这样当被感染文件执行的时候，实际上执行的是病毒文件。

(5) 链接病毒。这类病毒将自己隐藏在文件系统的某个地方，并使目录区中文件的开始簇指向病毒代码。这种感染方式的特点是每一个逻辑驱动器上只有一份病毒的副本。

6. 按照破坏能力分类

按照破坏能力可将病毒分为以下几种类型。

(1) 无害型：除了传染时减少磁盘的可用空间外，对系统没有其他影响。

(2) 无危险型：这类病毒仅仅是减少内存、显示图像、发出声音等。

(3) 危险型：这类病毒在计算机系统操作中造成严重的错误。

(4) 非常危险型：这类病毒删除程序，破坏数据，清除系统内存区和操作系统中重要的信息。

1.1.3 病毒的基本机理

病毒一般会有如下 4 种状态：

(1) 潜伏。病毒处于休眠状态，用户感觉不到病毒的存在。不过，有些病毒也可能没有潜伏期。

(2) 感染。病毒感染其他程序。一般感染需要一定的条件。

(3) 触发。病毒被某个条件激活，系统开始为其分配资源。

(4) 发作。病毒开始运行，对系统形成一些破坏。

为了实现上述 4 种存在状态间的变换，病毒程序需要有如图 1.3 所示的 3 个模块：引导模块、感染模块和表现(破坏)模块。

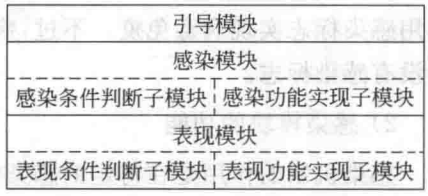

图 1.3 病毒的基本逻辑结构

1. 引导模块

1) 引导模块的基本功能

引导模块也称主控模块，主要实现如下功能。

(1) 将病毒装入内存，使感染和破坏(表现)模块处于活动的状态。

(2) 保护内存中的病毒代码不被覆盖。

(3) 设置病毒的触发条件。

2) 引导过程

(1) 检测运行环境，如操作系统类型、内存容量、现行区段、磁盘设置和显示器类型等。

(2) 驻留内存。自身的程序代码引入并驻留在内存中。

(3) 窃取控制权。取代或扩充系统原有功能，并窃取系统的控制权，设置病毒的激活条