21世纪

高等院校计算机系列教材

信息系统安全原理

张基温 编著

中国水利水电出版社
www.waterpub.com.cn

21世纪高等院校计算机系列教材

信息系统安全原理

张基温　编著

中国水利水电出版社

内 容 提 要

本书从应用的角度介绍计算机信息系统安全原理，并将有关内容按照如下体系梳理：第 1 篇攻防技术：内容包括恶意程序、网络攻击（黑客）、隔离技术（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；第 2 篇安全信任体系：内容包括加密与信息隐藏、认证、安全协议；第 3 篇安全体系结构和评估标准。

本书深入浅出、富有哲理，结构新颖、紧扣理论本质，适合学习，可以激发学习者的热情。书中还配有丰富的习题，供学习者自检。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和信息安全专业本科以及研究生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

信息系统安全原理 / 张基温编著. —北京：中国水利水电出版社，2005
（21 世纪高等院校计算机系列教材）
ISBN 7-5084-2493-X

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

中国版本图书馆 CIP 数据核字（2004）第 120740 号

书　　名	**信息系统安全原理**
作　　者	张基温　编著
出版　发行	中国水利水电出版社（北京市三里河路 6 号　100044） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）63202266（总机）、68331835（营销中心）、82562819（万水）
经　　售	全国各地新华书店和相关出版物销售网点
排　　版	北京万水电子信息有限公司
印　　刷	北京北医印刷厂
规　　格	787mm×1092mm　16 开本　17.25 印张　380 千字
版　　次	2005 年 1 月第 1 版　2005 年 1 月第 1 次印刷
印　　数	0001—5000 册
定　　价	26.00 元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

前　言

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；计算机信息系统具有虚拟性，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、风险、虚拟和困难，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。

这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，经反复探索，将安全理论梳理成如下三大类：

（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面向应用的安全技术，并且较为本质。这里，面向应用，是指不包含有关安全操作系统设计和实现的有关内容。

在内容的安排上，考虑了如下原则：

（1）适合教学：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）适合学习：将能引起兴趣的内容排在前面，以使学习者能有成就感；把安全体系结构和安全等级放在最后，不仅容易理解，而且也是对前面的内容的总结和提高。

（3）主次分明：重点内容详细介绍，次要内容只做一般介绍。

本书每章之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；
- 有些要自己查找资料；
- 有些要动手实验。

本人期望通过这些习题使学习者的自学能力、动手能力有较大的提高。

四川大学信息安全研究所方勇教授编写了书中的第 9.1 节。本书在编写过程中，还参考了大量资料。这些资料有的引自了国内外论文，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，但尚有许多疏漏，也受篇幅所限，恕不能一一列出。在此谨向有关作者致谢并表歉意。

在编写之后，我的研究生蒋中云、王玉斐、魏士婧、董瑜分头校读了有关章节，并制

作了课件。在此也向他们表示感谢。

计算机信息系统安全是一个涉及广泛、发展迅速的领域。尽管本人尽力想把它编写好，但客观和主观的能力所限，实在是心有余而力不足。本人希望读者和有关专家能不吝指正，以便适当的时候进一步修订。

张基温

2004 年 8 月 28 日

目　　录

第 2 篇 安全信任体系

第 3 篇 信息系统安全体系结构与评估标准

第1篇　信息系统攻击与防御

信息系统的危胁主要来自攻击。由于信息系统在社会中的重要地位，招致它不断受到花样翻新的攻击。“道高一尺，魔高一丈”，攻击与防御在相互的博弈中相得益彰，并且永不会完结。这里，只能介绍一些最基本的内容。

第 1 章　恶意程序及其防范

计算机病毒是恶意程序的一种。所谓恶意程序，是指一类特殊的程序，它们通常在用户不知晓也未授权的情况下潜入到计算机系统中来。恶意程序可以分为许多类型。图 1.1 所示为按照有无自我复制功能和需要不需要宿主对恶意程序的分类情形。

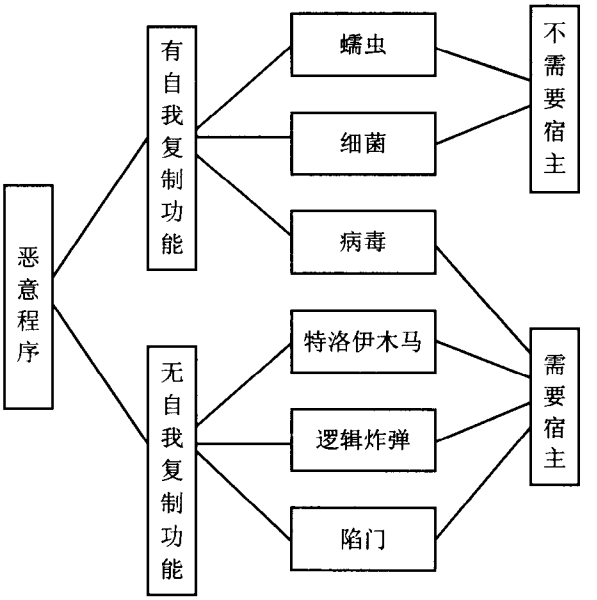

图 1.1　恶意程序及其分类

陷门（Trap Doors）是进入程序的一些秘密入口。陷门中有些是程序员为了进行调试和测试而预留的一些特权，有些则是系统漏洞。黑客也挖空心思地设计陷门，以便以特殊的、不经授权的方式进入系统。陷门通常寄生于某些程序（有宿主），但无自我复制功能。

逻辑炸弹是嵌入某些合法程序的一段代码，没有自我复制功能，在某些条件下会执行一个有害程序，造成一些破坏。

特洛伊木马是计算机网络中一种包含有害代码的有用或表面上有用的程序或过程，激活时产生有害行为。它们不具备自我复制功能。

细菌是以自我繁殖为主要目的的程序。

蠕虫是一种通过网络自我复制的恶意程序。通常人们也把它称为病毒的一种。因为，蠕虫一旦被激活，可以表现得像细菌和病毒，可以向系统注入特洛伊木马，或进行任何次数的破坏或毁灭行动。典型的蠕虫只会在内存维持一个活动副本。此外，蠕虫是一个独立程序，自身不改变任何其他程序，但可以携带具有改变其他程序的病毒。

计算机病毒是所有计算机用户在计算机安全问题上，经常碰到的问题。在 1999 年 Security Poral 的报告中，排在计算机安全问题第一位的是计算机病毒事件，其次是与计算机病毒关系极为密切的黑客问题。所以本章以病毒为主，介绍恶意程序的特点及其防治。

1.1　计算机病毒的概念

1.1.1　计算机病毒的定义

人类发明了工具，改变了世界，也改变了人类自己。自 20 世纪 40 年代起，计算技术与电子技术的结合，使推动人类进步的工具从体力升华到了智力。计算机的出现，将人类带进了信息时代，使人类生产力进入了一个特别的发展时期。

计算机的灵魂是程序。正是建立在微电子载体上的程序，才将计算机延伸到了人类社会的各个领域。“成也萧何，败也萧何”，人的智慧可以创造人类文明，也可以破坏人类已经创造的文明。随着计算机系统设计技术向社会各个领域急剧扩展，人们开发出了将人类带入信息时代的计算机程序的同时，也开发出了给计算机系统带来副作用的计算机病毒程序。

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。

在《中华人民共和国计算机信息系统安全保护条例》中，计算机病毒（Computer Virus）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破坏数据、影响计算机使用，并且能够自我复制的一组计算机指令或者程序代码”。

1.1.2　计算机病毒的特征

计算机病毒有一些与生物界中的病毒极为相似的特征，这也就是称其为病毒的缘由。主要有以下特征。

1.1.2.1　传染性和衍生性

病毒也是一种程序，它与其他程序的显著不同之处，就是它的传染性。与生物界中的病毒可以从一个生物体传播到另一个生物体一样，计算机病毒可以借助各种渠道从已经感染的计算机系统扩散到其他计算机系统。

早在 1949 年，计算机的先驱 Von Neumann 就在他的论文《复杂自动机组织论》中，提出了计算机程序在内存中自我复制的设想，勾画了病毒程序的蓝图。1977 年夏天，美国作家托马斯·捷·瑞安在其幻想小说《P-1 的青春》一书中构思了一种能够自我复制的计算机程序，第一次使用了“计算机病毒”的术语。所以自我复制应当是计算机病毒的主要特征。

20 世纪 60 年代初，美国贝尔实验室里，三个年轻的程序员编写了一个名为“磁芯大战”的游戏，游戏中通过复制自身来摆脱对方的控制，这就是计算机“病毒”的雏形。

1983 年美国计算机专家弗雷德·科恩博士研制出一种在运行过程中可以自我复制的具有破坏性的程序，并在同年 11 月召开的国际计算机安全学术研讨会，首次将病毒程序在

VAX/750 计算机上进行了实验。世界上第 1 个计算机病毒就这样出生在实验室中。

20 世纪 80 年代初，计算机病毒（如“巴基斯坦智囊”病毒）主要感染软盘的引导区。20 世纪 80 年代末，出现了感染硬盘的病毒（如“大麻”病毒）。20 世纪 90 年代初，出现了感染文件的病毒（如“Jerusalem，黑色 13 号星期五”病毒）。接着出现了引导区和文件型“双料”病毒，既感染磁盘引导区又感染可执行文件。20 世纪 90 年代中期，称为“病毒生产机”的软件开始出现，使病毒的传播不再是简单的自我复制，而是可以自动、轻易地自动生产出大量的“同族”新病毒。这些病毒代码长度各不相同，自我加密、解密的密钥也不相同，原文件头重要参数的保存地址不同，病毒的发作条件和现象也不同。

1995 年大量具有相同“遗传基因”的“同族”病毒的涌现，标志着“病毒生产机”软件已出现。目前国际上已有上百种“病毒生产机”软件。这种“病毒生产机”软件不用绞尽脑汁地去编程序，便可以轻易地自动生产出大量的“同族”新病毒。这些病毒代码长度各不相同，自我加密、解密的密钥也不相同，原文件头重要参数的保存地址不同，病毒的发作条件和现象也不同，但主体构造和原理基本相同。这就是病毒的衍生性。

与此同时，Internet 的发展，也为病毒的快速传播提供了方便途径。

1.1.2.2 潜伏性和隐蔽性

计算机病毒通常是由技术高超者编写的比较完美的、精巧严谨、短小精悍的程序。它们常常按照严格的秩序组织，与所在的系统网络环境相适应、相配合。病毒程序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。

除了不发作外，计算机病毒的潜伏还依赖于其隐蔽性。为了隐蔽，病毒通常非常短小（一般只有几百或 1K 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，使人不经过代码分析很难被发觉。

20 世纪 90 年代初，计算机病毒开始具有对抗机制。例如 Yankee Doole 病毒，当它发现有人用 Debug 工具跟踪它，就会自动从文件中逃走。此外还相继出现了一些能对自身进行简单加密的病毒，如 1366(DaLian)、1824(N64)、1741(Dong)、1100 等。加密的目的主要是防止跟踪或掩盖有关特征等。例如在内存有 1741 病毒时，用 DIR 列目录表，病毒会掩盖被感染文件所增加的字节数，使人看起来字节数很正常。

1.1.2.3 寄生性

1. 病毒的寄生场所

寄生是病毒的重要特征。计算机病毒一般寄生在以下地方：

（1）寄生在可执行程序中。一旦程序执行，病毒就被激活，病毒程序首先被执行并常驻内存，然后设置触发条件。感染的文件被执行后，病毒就会趁机感染下一个文件。

文件型病毒可以分为源码型病毒、嵌入型病毒和外壳型病毒。源码型病毒是用高级语言编写的，不进行编译、链接，就无法传染扩散。嵌入型病毒是嵌入在程序的中间，只能针对某些具体程序。外壳型病毒寄生在宿主程序的前面或后面，并修改程序的第 1 条指令，使病毒先于宿主程序执行，以便一执行宿主程序就传染一次。

（2）寄生在硬盘的主引导扇区中。这类病毒也称为引导型病毒。任何操作系统都有

自举过程，自举依靠引导模块进行，而操作系统的引导模块总是放在某个固定位置，这样系统每次启动就会在这个固定的地方再将引导模块读入内存，紧接着就执行它，来把操作系统读入内存，实现控制权的转接。引导型病毒程序就是利用这一点，它自身占据了引导扇区而将原来的引导扇区的内容和病毒的其他部分放到磁盘的其他空间，并将这些扇区标志为坏簇，不可写其他信息。这样，系统的一次初始化，就激活一次病毒，它首先将自身拷贝到内存，等待触发条件到来。

引导型病毒按其寄生对象，可以分为 MBR（主引导区）病毒和 BR（引导区）病毒。MBR 病毒也称为分区病毒，这类病毒寄生在硬盘分区主引导程序所占据的硬盘 0 头 0 柱面第 1 扇区，典型的有 Stoned（大麻）病毒、2708 病毒等。BR 病毒则寄生在硬盘逻辑 0 扇区或软盘 0 扇区（即 0 面 0 道的第 1 扇区），典型的有 Brain 病毒、小球病毒等。

2. 计算机病毒的寄生方式

（1）替代法。病毒程序用自己的全部或部分代码，替代磁盘引导扇区或文件中的全部或部分内容。

（2）链接法。病毒程序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。链接的位置可能在正常程序的首部、尾部或中间。

1.1.2.4　触发性

潜伏下来的计算机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。

1.1.2.5　非授权执行性

用户在调用一个程序时，常常就把系统的控制权交给这个程序并给它分配相应的系统资源，使程序的执行对用户是透明的。计算机病毒具有正常程序所具有的一切特性，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。

1.1.2.6　破坏性

计算机病毒的设计者进行病毒程序设计的目的就是为了攻击破坏。下面对病毒的破坏性进行分类介绍。

1. 病毒破坏的能力

按照病毒的破坏能力，可将病毒划分为以下几种。

- 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。
- 无危险型：这类病毒仅仅是减少内存、显示图像、发出声音及同类音响。
- 危险型：这类病毒在计算机系统操作中造成严重的错误。
- 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。

2. 病毒的入侵方式

（1）源代码嵌入攻击型。这类病毒主要入侵高级语言的源程序。病毒在源程序编译之前就插入进来，最后随源程序一起被编译成带毒可执行文件。这类带毒文件是极少数，因为这些病毒开发者不可能轻易得到那些软件开发公司编译前的源程序，并且入侵的方式