HZ BOOKS
华章教育

北京市高等教育精品教材立项项目

高等院校信息安全专业规划教材

国内权威操作系统安全专家编写，涵盖经典操作系统安全的理论和实践技术、业界开源操作系统安全的研究成果，以及最新的可信计算、系统虚拟化和云操作系统安全实践技术。

操作系统安全设计

Design for Operating System Security

沈晴霓 卿斯汉 ◎ 等编著

机械工业出版社
China Machine Press

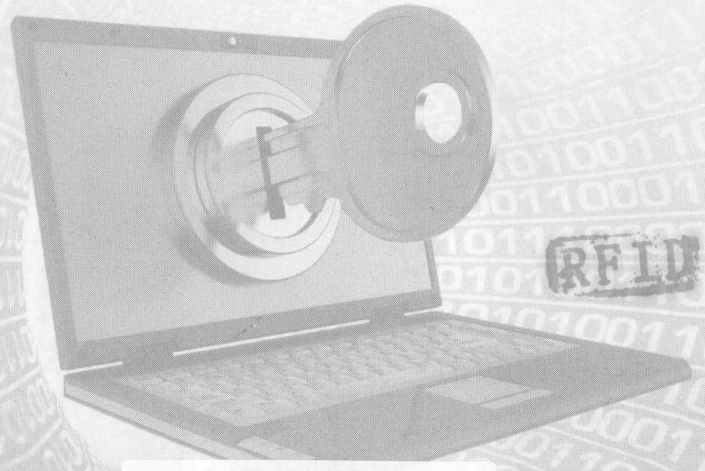
高等院校信息安全专业规划教材

北京市高等教育精品教材立项项目

操作系统安全设计

Design for Operating System Security

沈晴霓 卿斯汉 ◎ 等编著



机械工业出版社
China Machine Press

图书在版编目（CIP）数据

操作系统安全设计 / 沈晴霓等编著. —北京：机械工业出版社，2013.8
（高等院校信息安全专业规划教材）

ISBN 978-7-111-43215-9

I. 操… II. 沈… III. 操作系统－安全设计－高等学校－教材 IV. TP316

中国版本图书馆 CIP 数据核字（2013）第 154707 号

本书系统地介绍了经典的操作系统安全设计的相关理论和实践技术，并融入了最新的可信计算技术、系统虚拟化技术，以及未来的云操作系统进展及其安全实践。

本书内容由浅入深，分为“基础篇”、“理论篇”、“实践篇”和“趋势篇”四大部分。“基础篇”重点介绍操作系统基本安全概念、通用安全需求、安全标准和必要的安全机制等。“理论篇”重点介绍操作系统安全建模理论、安全体系结构设计思想，以及安全保证技术和测评方法等。“实践篇”重点介绍安全操作系统设计与实现技术的案例，以及基于安全操作系统的应用系统安全案例。“趋势篇”重点介绍最新的可信计算技术、系统虚拟化技术，以及操作系统进展及其安全实践。读者可以依据不同层面的需求灵活地选用相关部分的内容进行阅读。本书的每一章后面都附有习题和参考文献，便于读者对各章的内容进行思考和深入理解。

本书重点面向计算机、软件工程、信息安全等相关专业的高等院校本科生，也适用于高等院校和科研机构相关专业的硕士生和博士生，还可以作为相关学科领域科研人员、工程技术人员的参考用书。

机械工业出版社（北京市西城区百万庄大街 22 号 邮政编码 100037）
责任编辑：余 洁
北京瑞德印刷有限公司印刷
2013 年 9 月第 1 版第 1 次印刷
185mm×260mm · 24.25 印张
标准书号：ISBN 978-7-111-43215-9
定 价：59.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991 88361066 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

编委会

丛书序

经过数年的筹划与努力，信息安全系列丛书终于和广大读者见面了。

众所周知，进入21世纪以来，信息化对社会发展的影响日益深刻。全球信息化正在引发当今世界的深刻变革，重塑世界政治、经济、社会、文化和军事发展的新格局。

人们在享受信息化所带来的便利的同时，也不得不面对各种信息安全问题。信息安全是信息化的关键，各种天灾（如地震、洪水、飓风）和“人祸”（如网络故障、黑客入侵、病毒等）都会影响信息化进程。因此，在发展信息化的同时要重视信息安全，要在安全中发展，在发展中确保安全。

目前，世界各国都将信息安全视为国家安全的重要组成部分。党的十六届四中全会在《中共中央关于加强党的执政能力建设的决定》中明确提出：“坚决防范和打击各种敌对势力的渗透、颠覆和分裂活动，有效防范和应对来自国际经济领域的各种风险，确保国家的政治安全、经济安全、文化安全和信息安全”。党中央把信息安全和政治安全、经济安全、文化安全并列，作为我们国家四大安全内容之一，可见信息安全之重要，绝不能掉以轻心。近年来，我国在信息安全保障方面的工作逐步加强，制定并实施了国家信息安全战略，建立了信息安全管理体制和工作机制。基础信息网络和重要信息系统的安全防护水平明显提高，互联网信息安全管理进一步加强。

信息安全问题的解决，既要依靠技术的发展，更要重视人的作用。随着科技的进步，信息安全的概念和内涵不断发生变化，今天我们所说的信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等领域的交叉学科，各种保障信息安全的技术也不断推陈出新。我们应大力培养信息安全的专业人才，对从业人员进行技术、职业道德、法律等全方位的教育。同时，要普及信息安全教育，增强国民的信息安全意识，提高全民的信息化知识水平和防范意识。

面对社会对信息安全人才的迫切需求，国内已有几十所高校设立了信息安全专业，还有众多高校开设了信息安全相关的必修与选修课。为了有力地支持信息安全相关课程的教学，促进信息安全的科学研究，在机械工业出版社华章分社的精心策划与组织下，国内高校从事信息安全领域研究、教学的专家和教师共同编写了这套“高等院校信息安全专业规划教材”。这套丛书是各位作者多年教学、科研成果的结晶，其特点是理论与实践紧密结合、深入浅出、实例丰富，既包括基础知识，也反映最新科研成果与发展趋势。我深信，丛书的出版必将对信息安全知识的普及和推广、信息安全人才的培养、教学与科研产生积极影响并作出重要的贡献。

最后，作为本丛书的编委会主任，我对各位编委的努力工作、各位作者的辛勤劳动、机械工业出版社华章分社的大力支持表示衷心的感谢。

丛书编委会主任　卿斯汉

2009年6月

前言

信息安全基础设施的关键是操作系统安全，建设以我国自主知识产权为基础的安全操作系统，形成一系列基于安全操作系统的信息安全产品，是加强我国信息安全基础设施的根本保证。没有操作系统安全，就不可能真正解决数据库安全、网络安全和其他应用系统的安全问题。

自20世纪90年代以来，我们在操作系统安全相关领域进行了长期的研究与工程实践。2003年1月，在中国科学院科学出版基金的支持下，我们出版了国内第一部操作系统安全领域的专著——《操作系统安全导论》，全面介绍了操作系统的安全特性，总结了国际最新研究成果，也包括了当时我们研发成功的符合GB 17859第三级的安胜安全操作系统（V 3.0）的相关科研成果。为了满足我国高等学校和研究机构培养高素质信息安全人才的迫切需求，我们于2009年规划编写本书。本书融入了我们近七年来在北京大学软件与微电子学院的教学实践经验，以及近年来我们在可信计算、系统虚拟化、云安全技术等相关领域的最新科研实践成果。本书旨在通过对计算机、信息安全等相关学科的高校学生，特别是本科生的培养，进一步加强我国从事信息安全基础设施相关领域的研究和实践能力，提高我国在基础软件安全方面的国际竞争力。

本书内容由浅入深，分为“基础篇”、“理论篇”、“实践篇”和“趋势篇”四大部分，可以更好地适用于计算机、软件工程和信息安全相关专业本科生的教学，以及适合在读硕士生和博士生作为教材或参考书使用。

第一部分“基础篇”，包括第1～4章，重点介绍操作系统基本安全概念、通用安全需求、安全标准和必要的安全机制等。其中第1章（由卿斯汉、刘文清、沈晴霓编写）从操作系统面临的安全威胁着手，分析了操作系统通用安全需求及其在计算机信息系统的整体安全性中的重要性，介绍了操作系统安全等级划分与评测标准和相关术语。第2章（由卿斯汉、沈晴霓编写）介绍了操作系统安全的基本概念及预备知识。第3章（由沈晴霓、朱继锋编写）介绍了硬件安全、访问控制、可追究以及连续保护四大机制。第4章（由卿斯汉、刘文清编写）具体介绍了UNIX/Linux和Windows NT/XP等通用操作系统的安全机制。

第二部分“理论篇”，包括第5～7章，重点介绍操作系统安全建模理论、安全体系结构设计思想以及安全保证技术和方法等。其中第5章（由卿斯汉、沈晴霓编写）介绍安全策略和安全模型在操作系统安全中的重要地位、安全策略的分类，以及机密性、完整性、混合型/中立型和其他类型的经典安全策略和安全模型。第6章（由沈晴霓、赵志科编写）通过详细讲解两个典型实例（Flask安全体系结构和权能安全体系结构）以及LSM安全框架，说明安全体系结构的含义、类型、设计原则、设计目标和实现方法。第7章（由沈晴霓、温红子编写）探讨了安全保证的概念和方法，介绍了安全开发生命周期、安全测试技术、形式化规范与验证技术以及安全测评方法等。

第三部分“实践篇”，包括第 8 ～ 9 章，重点介绍我们自主研发的安胜安全操作系统的设计与实现案例，以及安全操作系统的应用实践。其中第 8 章（由卿斯汉、刘文清、沈晴霓编写）阐述了安胜安全操作系统的设计目标、总体结构，以及多级安全文件系统、隐蔽通道分析、安全加密文件系统、客体重用等机制的实现方法。第 9 章（由卿斯汉、张敏编写）介绍了基于安全操作系统的 Web 服务、防火墙以及数据库安全应用案例。

第四部分“趋势篇”，包括第 10 ～ 12 章，重点介绍最新的可信计算技术、系统虚拟化技术以及操作系统进展及其安全实践。其中第 10 章（由沈晴霓、靳远游编写）介绍可信计算的概念和技术，以及基于 TPM/TCM 可信操作系统的核心技术。第 11 章（由沈晴霓编写）介绍了系统虚拟化技术分类、实现方法，以及当前主流的系统虚拟化软件，从虚拟化平台技术及其安全机制、虚拟可信平台架构及其安全机制的角度帮助读者了解虚拟化技术及其安全机制和可信机制。第 12 章（由沈晴霓编写）介绍随着安全问题的日益突出和云计算新技术的出现，业界目前十分关注的 SELinux、Solaris 10、Windows Vista/Windows 7，以及未来云操作系统，包括 Google Chrome OS、Windows Azure、Android OS 的发展及其安全考虑。

在本书的编写过程中，我们特别感谢北京大学软件与微电子学院信息安全系的可信虚拟化研究组（TVG）和原中科院软件所信息安全工程研究中心的安全操作系统研究组的所有成员，书中涉及的许多科研成果是在大家的共同努力下完成的。在此，我们特别感谢刘文清博士、温红子博士、刘海峰博士、朱继锋博士、季庆光博士、李丽萍博士、唐柳英博士、沈建军博士、赵志科硕士、邢常亮硕士、张可新硕士等，特别感谢倪惜珍研究员、贺也平研究员、张敏副研究员等。现在在英国牛津大学的阮安邦博士生、美国耶鲁大学的古亮博士等，以及目前已经毕业的孙鹏飞、李扬威、陈莹、靳远游、魏磊、石磊、李钊、禹熹、易晓磊、袁傲、马喆等同学，感谢他们在北京大学攻读硕士或博士学位期间，曾参与完成相关领域的科研实践工作，为本书的完成奠定了良好的基础。最后，感谢参与本书相关文献检索和初期整理工作的束锐、李才、周志轩、赵原、刘龙、万冕、王俊清，以及张壮壮、周建国、张智、黄淮等硕士生，他们为本书的初期工作花费了大量的时间和付出了许多的努力。

本书的出版得到国家自然科学基金项目（60083007，60573042，60873238，60970135，61073156，61170282，61232005）、国家重点基础研究发展规划项目（G1999035810）和国家科技支撑计划基金项目（2008BAH33B02）的支持，也得到北京大学“教学新思路”建设项目、北京大学软件与微电子学院“精品课程”建设项目，以及 Intel UPO Security Curriculum 全球项目、华为高校基金项目的支持，在此表示感谢。我们还特别感谢本丛书的编委会，他们对本书的架构与组织提出了宝贵的建议。最后，我们感谢机械工业出版社华章公司的朱劼、佘洁女士，她们为本书的顺利出版付出了大量心血。

尽管我们仔细审核了全书内容，并试图消除任何细节上的错误，但是受我们的水平和时间的限制，如书中出现任何错误、疏漏和不足，敬请广大读者帮助指正，非常感谢！

沈晴霓　卿斯汉

2013 年 2 月 16 日

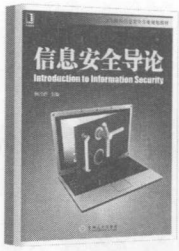
教学建议

教学章节	教学要求	课时（学时）
第 1 章 引言	了解操作系统安全威胁和安全需求 了解操作系统安全的重要性 了解国内外安全操作系统发展历史与现状 掌握计算机系统安全等级划分与评测标准	2～4
第 2 章 基本概念	掌握系统边界和安全周界的划分思想 掌握可信软件和不可信软件的划分思想 掌握访问控制思想和引用监控器的概念 掌握构建安全的三大要素：安全策略、安全机制和安全保证的基本概念和类型 掌握可信计算基的含义	4
第 3 章 操作系统基本安全机制	了解存储、运行、I/O 等硬件安全机制 掌握自主访问控制、强制访问控制、客体重用等访问控制机制 掌握标识与鉴别、可信通路、安全审计等可追究机制 掌握系统完整性、隐蔽通道分析、最小特权管理、可信恢复等连续保护机制	8
第 4 章 通用操作系统安全机制	了解 UNIX/Linux 操作系统体系结构 掌握 UNIX/Linux 操作系统的安全机制 了解 Windows NT/XP 操作系统体系结构 了解 Windows NT/XP 操作系统的安全机制	4～6
第 5 章 安全策略与安全模型	了解安全策略的类型 了解安全模型的作用、特点、一般开发方法 掌握经典机密性模型——BLP 模型思想和表示 掌握经典完整性模型——Biba 模型思想和表示 掌握中国墙、RBAC 和 DTE 等混合模型的思想	4～6
第 6 章 安全体系结构	了解安全体系结构的概念、设计原则和目标 了解通用访问控制框架（GFAC）的设计思想 掌握经典 Flask 安全体系结构的设计思想 掌握 LSM 安全框架的实现方法 了解权能安全体系结构的设计思想（选讲）	6～8
第 7 章 安全保证技术	了解安全保证的概念和必要性等 掌握安全开发生命周期 了解安全测试技术 了解形式化规范与验证技术（选讲） 了解操作系统安全测评方法	2～4

（续）

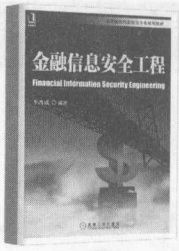
教学章节	教学要求	课时（学时）
第 8 章 安全操作系统设计与实现技术	了解安全系统设计原则、一般开发过程 掌握安全操作系统的常用开发方法，包括虚拟机法、改进 / 增强法、仿真法等 了解安全操作系统设计与实现案例技术 掌握多级分层文件系统的设计 掌握隐蔽存储通道的分析和场景构造方法	6 ～ 8
第 9 章 安全操作系统的应用	了解安全操作系统与 Web 服务器安全的关系 了解安全操作系统与防火墙安全的关系（选讲） 了解安全操作系统与数据库安全的关系（选讲）	2
第 10 章 可信计算技术	了解可信计算概念、形成历程、TCG 组织等 了解 TPM、TCM 与 TPM.next 的关系 掌握可信平台的信任传递、完整性度量、完整性报告、证书机制和密钥管理等机制 了解基于 TPM/TCM 的可信操作系统问题、要求和机制（选讲）	4 ～ 6
第 11 章 系统虚拟化技术	了解系统虚拟化技术分类、实现和硬件支持 掌握虚拟机监控器的安全体系结构 了解虚拟机迁移安全机制、虚拟机安全监控技术、虚拟机之间隐蔽通道分析、I/O 隔离技术等（选讲） 了解 VPWG 及虚拟可信平台技术进展（选讲）	4 ～ 6
第 12 章 操作系统进展及其安全实践（选讲）	掌握 SELinux 实现的安全策略及其基本配置方法 了解在操作系统及其安全应用方面的一些新进展，包括 Solaris、Chrome OS、Azure、Android 等系统（选讲）	2 ～ 4

推荐阅读



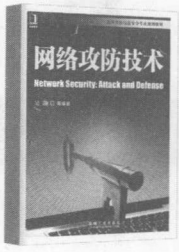
信息安全导论

作者：何泾沙 ISBN：978-7-111-36272-2 定价：33.00元



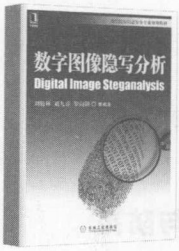
金融信息安全工程

作者：李改成 ISBN：978-7-111-28262-4 定价：35.00元



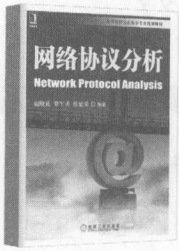
网络攻防技术

作者：吴灏 ISBN：978-7-111-27632-6 定价：29.00元



数字图像隐写分析

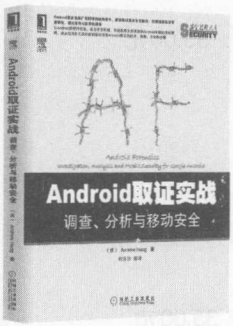
作者：刘粉林 刘九芬 罗向阳 ISBN：978-7-111-30517-07 定价：29.00元

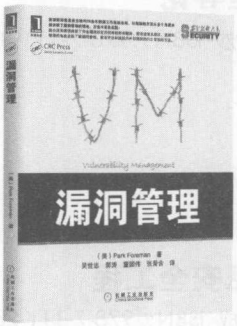


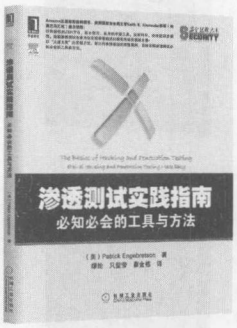
网络协议分析

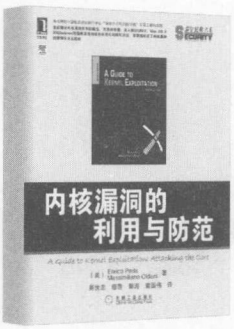
作者：寇晓蕤 罗军勇 蔡延荣 ISBN：978-7-111-26832-1 定价：33.00元

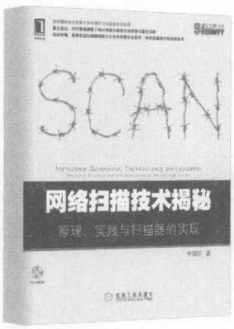
推荐阅读

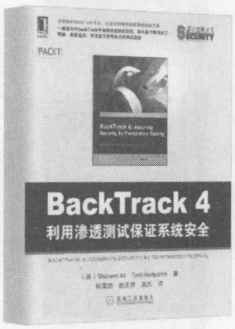












■ **Android取证实战：调查、分析与移动安全**
作者：Andrew hoog
ISBN：978-7-111-42199-3
定价：69.00元

■ **漏洞管理**
作者：Park Foreman
ISBN：978-7-111-40137-7
定价：69.00元

■ **渗透测试实践指南：必知必会的工具与方法战**
作者：Patrick Engebretson
ISBN：978-7-111-40141-4
定价：49.00元

■ **内核漏洞的利用与防范**
作者：Enrico Perla 等
ISBN：978-7-111-37429-9
定价：79.00元

■ **网络扫描技术揭秘：原理、实践与扫描器的实现**
作者：李瑞民
ISBN：978-7-111-36532-7
定价：79.00元

■ **BackTrack 4：利用渗透测试保证系统安全**
作者：Shakeel Ali
ISBN：978-7-111-36643-0
定价：59.00元

目录

第二部分 理论篇

第三部分 实践篇

第四部分 趋势篇

第一部分 基 础 篇

Chapter

第1章 引 言

1.1 操作系统安全威胁与安全需求

进入21世纪后，IT业的发展遇到了一个比较严酷的调整期，人们都在思考一个问题——IT业怎么了？其实除了过度投资等原因之外，另一个根本原因在于，以计算机技术为核心的IT业还没有完全具备解决信息处理中安全问题的能力。可以说，信息安全技术的发展将从根本上影响和制约信息技术的进一步发展。

作为信息技术最重要的基石，功能日益完备的操作系统正在迅速改变人类生活的旧有模式。一方面，操作系统带来的舒适、便捷让人们面对各种事务和问题时更为强大；而另一方面，操作系统中持续激增的各种信息安全问题，也让人们在遭受威胁时更为脆弱。而人们认识到信息安全问题通常是从对系统所遭到的各种成功或者未成功的入侵攻击的威胁开始的，这些威胁大多通过挖掘系统的弱点或者缺陷来实现，有记录的第一次这样的大规模攻击当属1988年的“蠕虫”事件。同时AT&T实验室的S.Bellovin博士曾对CERT（Computer Emergency Response Term，计算机安全响应组）提供的安全报告进行过分析，结果表明很多安全问题源于操作系统的安全脆弱性。随着网络技术的飞速发展，信息资源的共享程度进一步加强，特别是因特网的大规模应用以及金融、移动通信等重要网络的接入，越来越多的系统遭到入侵攻击的威胁。所以下面首先介绍操作系统面临的主要安全威胁类型。

1.1.1 安全威胁类型

1. 计算机病毒

计算机病毒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。计算机病毒具有以下基本特点：

1）隐蔽性：病毒程序代码驻存在磁盘等介质上，无法以操作系统提供的文件管理方法观察到。有的病毒程序设计得非常巧妙，甚至用一般的系统分析软件工具都无法发现它的存在。

2）传染性：当用户利用磁盘片、网络等载体交换信息时，病毒程序趁机以用户不能察觉的方式随之传播。即使在同一部计算机上，病毒程序也能在磁盘的不同区域间传播，附着到多个文件上。

3）潜伏性：病毒程序感染正常的计算机之后，一般不会立即发作，而是潜伏下来，等到激发条件（如日期、时间、特定的字符串等）满足时才会产生破坏作用。

4）破坏性：当病毒发作时，通常会在屏幕上输出一些不正常的信息，同时破坏磁盘上的数据文件和程序。如果是开机型病毒，可能会使计算机无法启动。有些“良性”病毒不破坏系统内现存的信息，只是大量地侵占磁盘存储空间，或使计算机运行速度变慢，或造成网络堵塞。

2. 蠕虫

蠕虫类似于计算机病毒，是一种能够自我复制的计算机程序。蠕虫攻击带来的破坏可能与计算机病毒一样严重，尤其是在没有及时发觉的情况下。蠕虫可能会执行垃圾代码以发动分散式阻断服务攻击，降低计算机的执行效率，影响计算机的使用；还可以侵入合法数据处理程序，更改或破坏这些数据。

3. 逻辑炸弹

逻辑炸弹指附着在某些合法程序上的恶意代码，其通常处于潜伏状态，但在特定的逻辑条件满足的情况下会激活和执行，对系统功能造成严重破坏。一般逻辑炸弹都被添加到被感染程序的起始处，通常要检查各种条件，看是否满足运行“炸弹”的条件。如果没有控制权就归还给主程序，逻辑炸弹仍然安静地等待。当设定的爆炸条件被满足后，逻辑炸弹的其余代码就会执行。此时它通常造成终止机器、制造刺耳噪声、更改视频显示、破坏磁盘上的数据、利用硬件缺点引发硬件失效、导致磁盘异常、使操作系统运行速度减慢或崩溃等危害。它也可以通过写入非法的值来控制视频卡的端口，使监视功能失败、使键盘失效、破坏磁盘以及释放出更多逻辑炸弹和/或病毒（间接攻击）。逻辑炸弹不能复制自身，不能感染其他程序，但这些攻击已经使它成为一种极具破坏性的恶意代码类型。

逻辑炸弹具有多种触发方式：计数器触发器、时间触发器、复制触发器（当病毒复制数量达到某个设定值时激活）、磁盘空间触发器、视频模式触发器（当视频处于某个设定模式或从设定模式改变时激活）、基本输入输出系统（BIOS）触发器、只读内存（ROM）触发器、键盘触发器、反病毒触发器等。

4. 特洛伊木马

特洛伊木马是一段计算机程序，表面上在执行合法功能，实际上却完成了用户不曾意料到的非法功能。受骗者是程序的用户，入侵者是这段程序的开发者。特洛伊木马必须具有以下几项功能才能成功地入侵计算机系统：

1）入侵者要写一段程序进行非法操作，程序的行为方式不会引起用户的怀疑。

2）必须设计出某种策略诱使受骗者接受这段程序。

3）必须使受骗者运行该程序。

4）入侵者必须通过某种手段回收由特洛伊木马发作为他带来的实际利益。

特洛伊木马程序与病毒程序不同，是一个独立的应用程序，不具备自我复制能力。但它同病毒程序一样，具有潜伏性，且常常具有更大的欺骗性和危害性。特洛伊木马也可能包含