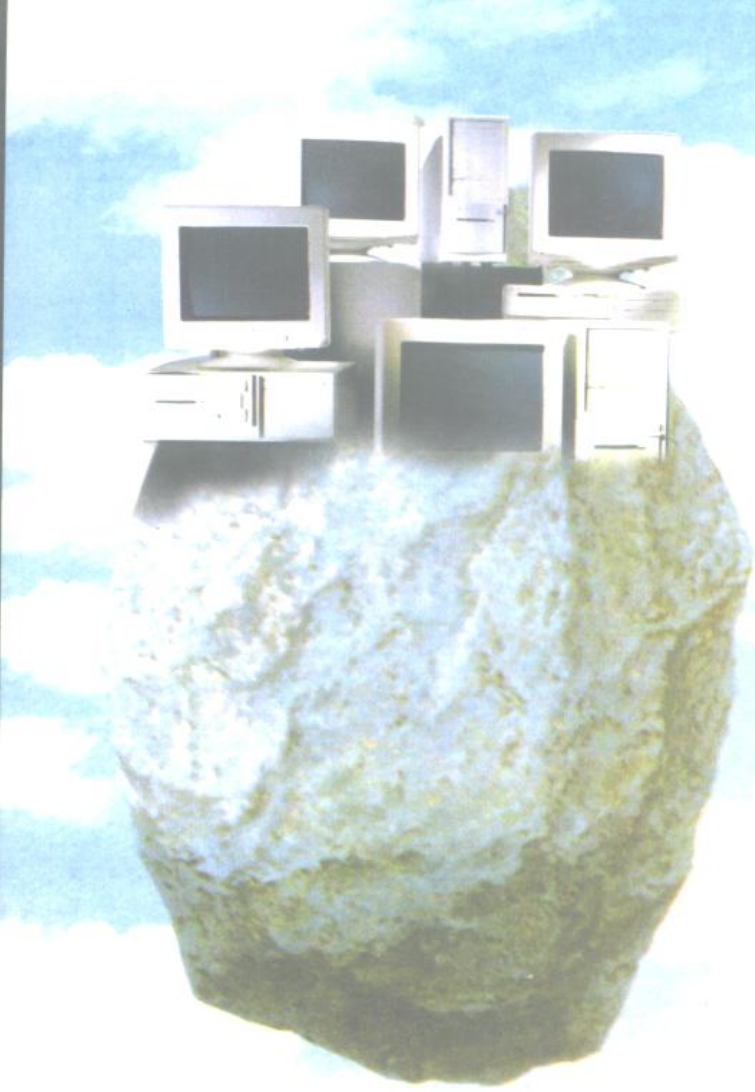
计算机应用系统安全



叶 红 编著

清华大学出版社

计算机应用系统安全要则

叶 红 编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书从保证计算机应用系统安全的角度出发，论述了计算机安全的概念和保证计算机系统安全的技术和手段。主要内容包括：在计算机应用系统生命周期的不同阶段应采取的安全措施、安全管理、安全评估和风险分析、安全验证与认定、网络安全、计算机安全标准与立法等。附录中收录了我国正式颁布的计算机安全方面的法规和标准(摘要)。

本书既可作为广大计算机应用人员的自学用书，也可作为计算机安全工程设计的参考用书。

图书在版编目(CIP)数据

计算机应用系统安全要则/叶红编著. —北京：清华大学出版社，1998

ISBN 7-302-02789-7

Ⅰ. 计… Ⅱ. 叶… Ⅲ. 电子计算机-安全技术 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(97)第 29005 号

出版者：清华大学出版社（北京清华大学校内，邮编 100084）
因特网地址：www.tup.tsinghua.edu.cn
印刷者：北京清华园胶印厂
发行者：新华书店总店北京科技发行所
开　本：787×1092 1/32　印张：6 7/8　字数：177 千字
版　次：1998 年 2 月 第 1 版　1998 年 2 月 第 1 次印刷
书　号：ISBN 7-302-02789-7/TP・1433
印　数：0001～5000
定　价：7.80 元

序

随着我国信息化建设的推进，计算机在社会、经济各领域甚至家庭中的应用迅速发展，再加上国际发展趋势以及互联网的不断普及，我国以计算机和通信技术为主要内容的现代信息技术的应用进入了一个新阶段。一批大的计算机应用系统相继投入运行，另有许多系统在建设中，这将对我国国民经济与社会发展产生深远影响。

与此同时，我们也看到，有一个问题在困扰着人们，那就是计算机系统的安全问题。目前，这一问题已引起我国有关部门、各级领导和广大业界人士的重视，并为此做了大量工作，包括舆论工作。已有不少这方面的文章见于各种媒体，但是，较全面、系统地论述计算机安全的书籍并不多。应该说，编写安全方面的书籍是有一定难度的：首先，计算机安全是一个新领域，还有待完善和发展，面对信息技术的迅速发展和变化，面对计算机应用深入、普及的迅猛趋势，了解并掌握不断出现的新问题是很困难的；其次，计算机安全是一个非常复杂的问题，涉及广泛的学科与领域，包括社会科学、自然科学与技术、国家法律、行政管理，仅就技术本身而言也跨越了许多学科；还有人们的认识问题和在我国的实践程度以及其他特殊因素等。这也许就是有关计算机系统安全方面书籍较少的原因吧。

因此，当我看到叶红编著的《计算机应用系统安全要则》一书时很高兴。这本书可以从某种程度上填补上述不足。

初读该书，有几点感受，或者说是该书的特点吧。

其一，该书除较全面地论述了计算机安全涉及的方方面面（包括基本概念、特点、主要安全技术与方法、评估、验证以及标准与立法等）外，整体上是从应用系统安全的角度出发，按计算机应用系统开发各阶段分别详细论述了每阶段在安全方面该做什么和怎样做。这种思路和做法是很重要的，也是很有意义的。目前，国内不少已经运行或正在设计中的应用系统，不是从一开始就把安全保障放到系统建设的各阶段中，而是到运行发生问题时再来补救。实际上，在这个时候要使系统具有同样的安全程度所遇到的困难和所花费的代价，比把安全保障放在系统全过程中给以考虑要大得多。

其二，该书从安全技术与管理有机结合的角度，对安全管理给予了详细而又具体的论述，这是很有价值的，也是已见到的同类书中较少的。国内外大量的经验与实践表明，保证系统安全要从法律、行政管理、技术手段等方面综合采取措施才最有效。技术不能作为全部，甚至对有些系统来说连“大部分工作”都不能说，在这方面管理是相当关键的一环。而对于我国目前的具体情况，强调并重视管理尤为重要，这也可能是一种用较少代价而取得较好效果的办法。

其三，该书的论述具体、实用，对于计算机安全方面的书籍来讲是很不容易的。

总之，我认为这是一本值得一读的好书，愿向广大读者推荐。

李正男

1997 年 10 月

前　言

计算机系统安全是计算机领域的一门新兴学科。随着计算机的迅速普及和发展，计算机应用已渗透到社会的各个方面。与此同时，人们对它的依赖性也日益增强。但是，你是否知道，计算机系统并不安全，甚至不堪一击。因此，对于花费了大量人力、财力、物力和时间，并维系着国家安全、人民利益的计算机系统，保证它的安全至关重要，这也是每一个系统设计者和管理者以及使用者共同关心的问题。

撰写本书的目的在于让人们认识计算机安全的重要性，了解计算机安全的基本概念和解决安全问题的技术方法及手段。本书还介绍了国内外在计算机安全标准和立法方面的现状及发展，以便让读者对计算机安全的历史和发展有所了解。

全书内容包括：

第 1 章概述计算机安全的基本概念。

第 2 章叙述保障计算机应用系统安全的技术和手段。

第 3 章至第 6 章论述了在应用系统生命周期的各个阶段如何保证安全以及应采取的安全措施。

第 7 章强调安全管理的重要性，并介绍了在各个环节上的管理内容和管理手段。

第 8 章和第 9 章介绍了对计算机系统的安全评估和风险分析方法，以及如何对一个已建立的系统进行安全验证和认定。

第 10 章概述网络安全。

第 11 章描述了国内外计算机安全标准与立法的现状及发展。

附录中收集了我国正式颁布和发表的计算机安全方面的法规和标准(摘要)。

中国计算机学会计算机安全专业委员会副主任、国家信息中心副主任李正男先生在本书的编写过程中给予了大力支持和帮助,并通篇审阅,在此谨表示感谢。

限于作者的水平,书中会有不当之处,敬请指正。

作 者

1997 年 10 月

目 录

第1章 计算机安全概论

信息时代的到来，使计算机应用更加广泛、深入。电子信息技术已经渗透到人们的日常生活中，它改变了传统的事务处理方式，对社会的进步和发展起着推波助澜的作用。但是，当人们充分享受计算机带来的各种便利和快捷的同时，你是否会想到计算机并不安全，而且，随着计算机应用的发展和全社会计算机应用水平的提高，不安全因素会越来越多。计算机"黑客"通过非法手段，滥用信息资源，干扰他人正常活动，窃取钱财，扰乱社会安定甚至危害国家安全的事件已经摆在我们的面前。因此，普及计算机安全知识，增强全民的计算机安全意识，保护计算机应用事业健康发展迫在眉睫。本章将介绍计算机安全的一些基本概念。

1.1 计算机安全的概念

1.1.1 什么是计算机安全

计算机安全强调的是计算机信息系统的安全运行，即保障计算机及其相关的和配套的设备、设施(含网络)的安全，保障运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全运行。一个计算机信息系统运行涉及许多因素(如人、设备(含软件、设施))和诸多环节(如数据录入、数据处理、存储、传输等)。计算机安全的

本质就是要保证这些因素和环节在整个系统运行过程中正常发挥它们的作用，使系统安全可靠地工作。

计算机安全反映的是计算机系统对于由于系统故障、人为失误、恶意破坏以及各种自然灾害而引起正常业务中断的抵抗能力，它包括三个关键要点：首先，计算机的安全性是一个相对量，不是一个要求达到的绝对量，因为不同用途的应用系统有不同的安全要求，追求不切合实际的高安全性不仅会造成浪费，还会引起操作上的不便；其次，对计算机的安全性，考虑的是四个同等重要的方面，即泄露、修改信息、破坏设备和设施、中断业务；第三，上述四个方面不只局限于数据上，还应考虑硬件和相关的物理设施。

“计算机安全”一词的含义概括起来包括以下三个方面的内容：

1. 完整性

程序和数据的存在状态应该与原文件中的存在状态相同，信息不能被非法修改，无论这种修改是偶然无意的还是蓄谋恶意的。完整性反映的是信息的精确度与可靠性。

完整性技术可分为软件完整性保护和数据完整性保护。一个计算机系统的庞大功能是由成千上万条语句和指令来完成的，软件设计的灵活性和可变性为系统的开发和更新提供了方便，但是同时正是这种特性给系统的安全性带来了严重威胁。假如软件的设计者存有某种阴谋，他可以方便地在程序中留下陷阱，以期达到他预想的结果。计算机病毒就是利用软件完整性的缺陷，在正常秩序中附加了一部分病毒程序代码，在系统或应用程序运行过程中进行自身繁殖、传染、改写系统参数，最终导致系统瘫痪、数据丢失。

另外，软件的设计方案及源代码的泄露也为攻击系统提供了机会。有预谋的程序员可以对软件进行难以检测的修改。如果将特洛伊木马引入系统软件，就很可能导致机密信息非法泄露。

目前，数据完整性问题也是广大计算机用户普遍关心的问题。所谓数据完整性保护是指存储在计算机系统中或在计算机系统间传输的数据不被非法篡改或遭意外事故的破坏，以保证数据的完整。数据完整性遭破坏一般由以下原因造成：

(1) 人为蓄意破坏。

(2) 意外事故造成的破坏，如机器故障、突然断电、强电磁干扰等。

(3) 应用程序错误。

(4) 存储介质损坏。

2. 可用性

可用性是指无论何时，只要用户需要，信息系统必须是可用的，也就是说计算机信息系统不能拒绝服务。

可用性涉及的因素很多，如环境因素——由于温度、湿度或供电系统不合要求导致硬件故障；系统因素——系统内部的某一功能(软件、硬件)发生故障或错误时，自动纠错或自动恢复能力差，使得系统挂起；人为因素——无意的操作失误和蓄意的破坏都会使系统瘫痪。

可用性在实时控制系统中显得尤为重要，例如空中管制、航天飞行、军事工程、证券交易等，在这些系统中即便是瞬间的系统故障都可能带来难以想像的损失，甚至付出生命的代价。

解决可用性问题可以通过提高系统部件的准确性、双机