国外著名高等院校
信息科学与技术优秀教材

WILEY

计算机安全

COMPUTER SECURITY

〔英〕Dieter Gollmann 著
华蓓 蒋凡 史杏荣 杨寿保 译
杨寿保 审校

人民邮电出版社
POSTS & TELECOM PRESS

国外著名高等院校信息科学与技术优秀教材

计算机安全

[英] Dieter Gollmann 著

华 蓓 蒋 凡 史杏荣 杨寿保 译

杨寿保 审校

人民邮电出版社

图书在版编目（CIP）数据

计算机安全 /（英）戈尔曼（Gollmann, D. ）著；华蓓等译. —北京：人民邮电出版社，2003.12
国外著名高等院校信息科学与技术优秀教材
ISBN 7-115-11811-6

Ⅰ. 计… Ⅱ. ①戈… ②华… Ⅲ. 电子计算机—安全技术—高等学校—教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2003）第 091534 号

版 权 声 明

国外著名高等院校信息科学与技术优秀教材
计算机安全

◆ 著 [英] Dieter Gollmann
译 华 蓓 蒋 凡 史杏荣 杨寿保
审 校 杨寿保
责任编辑 李 际

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
读者热线 010-67132705
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：17.75
字数：495 千字 2003 年 12 月第 1 版
印数：1-4 000 册 2003 年 12 月北京第 1 次印刷

著作权合同登记 图字：01 - 2003 - 0669 号
ISBN 7-115-11811-6/TP • 3732
定价：32.00 元

内容提要

这是一本侧重从技术的角度上讲授计算机安全（*computer security*）的教科书。全书分成四部分：第一部分“基础知识”，介绍了身份识别和认证、访问控制、安全模型，以及安全内核；第二部分“实践”，介绍了 Unix 和 Windows NT 安全、安全问题所在，以及安全评估；第三部分“分布式系统”，介绍了分布式系统安全、Web 站点安全、密码学，以及网络安全；最后是理论部分，介绍数据库安全、多级安全数据库、并发控制和多级安全，以及面向对象的安全。

本书内容丰富，深入浅出，理论与实践结合，覆盖了从基本的计算机安全概念、安全模型和安全理论，到具体的安全策略、安全实践和安全评估。每章都有丰富的习题和进一步阅读的建议及电子资源的出处，帮助读者消化和巩固所学内容，并启发读者思考。因此本书适合高等院校计算机科学技术相关专业的高年级本科生和研究生作选修课教材，特别适合新设信息安全专业的本科生、研究生作专业必修课教材。本书也可供从事计算机和信息系统安全的工程技术人员作自学教材和工作参考书。

世界著名高校教师对本书的评价

“这是一本我寻求了多年的好书。”

——Viiveke Fåk，瑞典林科平大学

“这是一本优秀的教科书，无疑是针对计算机科学系的学生写的。”

——John Biggam，英国格拉斯哥·卡勒多尼大学

“……这是作为理论的或职业的计算机系统安全入门课程的主要教科书……”

——Sokratis K. Katsikas 教授，希腊 Aegean 大学

“这是一本极具价值的书，特别针对那些计算机专业人员，他们不是专家，但是在这方面有合理的问题和需要。对于每一个计算机管理者和软件设计者的藏书室来说，它绝对是一本受欢迎的新书……，我想你们有了一本好书，我从心底里推荐它付梓出版。”

——J. Seberry 教授，澳大利亚卧龙岗大学

“我特别喜欢这本书关于最新出现的 Windows NT、CORBA 和 Java 安全技术的介绍。本书提供了其他类似的计算机安全书籍所不具备的附加值。”

——Rolf Oppliger，瑞士联邦政府信息技术和系统办公室

“作为设计计算机安全课程并在过去四年中一直给最后一年本科生授课的教授，我印象最深刻的是：这是一本在计算机安全方面培养学生和专业人员的好课本。”

——Simon Foley，爱尔兰 College Cork 大学

“这本书应该出现在每一个使用或实施计算机安全的计算机安全专业人员和计算机及 Internet 用户的书架上。”

——Yong Fei Han，新加坡国立大学

译者序

计算机技术和网络技术是当今世界发展最快，也是最具影响力的技术。计算机技术的突飞猛进，因特网的迅速成长，极大地推动了世界的进步。随着计算机在人类生活中各个领域的广泛应用，计算机系统的安全问题也越来越引起世界各国的广泛关注。计算机不断遭到各种非法入侵，计算机病毒不断产生和传播，重要数据资源遭到破坏或丢失，给计算机信息系统的正常运行造成了严重的危害，给经济活动带来巨大损失，甚至危及国家和地区的安全。因此，普及计算机信息系统安全知识，提高信息安全防范意识，培养计算机与网络安全的专门人才，已经成为当务之急。许多学校为研究生开设了计算机和网络安全课程，有些学校已经设立了信息安全专业，从本科生开始，培养信息安全专门人才。

我们根据多年的教学实践和信息安全技术的发展趋势，从众多的国外著名高校的优秀教材中选择了本书进行翻译，介绍给读者。本书的作者 Dieter Gollmann 从 1992 年到 1997 年一直是伦敦大学 Royal Holloway 信息安全中心硕士课程的设计主管，本书就是从该研究生教育的几门课程的教学中逐渐形成的。Dieter Gollmann 后来作为信息安全研究学者加入了设在英国剑桥的微软研究院。

本书的第一部分从基本的定义和概念开始，描述计算机系统核心部分的安全机制，以及为使用在系统其他部分的技术提供基础。第二部分分析了诸如 UNIX 和 Windows NT 操作系统中的安全特性，对安全漏洞进行分类，并引进了安全评估的有关主题。第三部分专注于分布式系统的安全问题，如网络(还有 Web)的安全，并把密码学作为这种环境里的基本技术。本书最后一部分是围绕着数据库安全来组织的，讨论了多级安全，分析在特定设置状态下的安全问题。本书内容丰富，深入浅出，理论与实践结合。每章最后都有练习题，以及关于进一步阅读的建议，包括许多电子资源的出处，有助于学生复习和巩固所学知识，启发学生思考，进一步自学和提高。

本书可以用于自学和课堂教学，适合计算机科学、工程或相关学科更高级的安全课程的学生使用。因此，本书可作为高等院校计算机科学技术相关专业的高年级本科生和研究生的选修课教

材，特别适合新设信息安全专业的本科生、研究生作专业必修课教材。本书也可供从事计算机和信息系统安全的工程技术人员作自学教材和工作参考书。

参加本书翻译的人员有：

华　蓓，中国科学技术大学计算机科学技术系副教授(1～5 章)

蒋　凡，中国科学技术大学计算机科学技术系教授(6～9 章)

史杏荣，中国科学技术大学电子科学与信息工程系教授(10～13 章)

杨寿保，中国科学技术大学计算机科学技术系教授、博士生导师(14～17 章)

全书由杨寿保负责审校和统稿。中国科技大学计算机科学技术系的研究生杨法娜同学参加了部分翻译和审校工作，谨此表示衷心感谢。

最后，我们要特别感谢人民邮电出版社计算机图书第二出版中心的编辑同志。他们为本书的翻译和审校工作提出了许多具体的建议和指导性意见，并以他们的辛勤工作为本书译稿精心设计与排版，才使本书中译本得以与读者早日见面。

限于译者的水平，译文中的错误和疏漏在所难免，敬请读者批评指正。

杨寿保

2003 年 7 月于中国科学技术大学

前　言

这本书源于我给一年级研究生上信息安全课程的讲义。在这个研究生项目第一年里，当讨论到涉及工业的实例时，负责安全的主管强调了明确说明安全目标的重要性，这些目标往往是具体项目不会有意识地提供的。因此，

- 本书不是一本计算机安全手册。
- 本书不是一本计算机安全的百科全书。
- 本书不是一本计算机安全发展史。

当然，这本书将会谈及在计算机安全发展史中的事件。它会覆盖相当广的背景知识，指出在这个领域中更深层次的问题，同时我希望，计算机安全实践者们将从中找到一些有用的想法和内容。然而，这是第一次，也是首部将计算机安全作为教科书来编写的书籍。这本书殷切地希望给那些已经有计算机科学背景知识的学生，提供关于评估和比较这些安全产品技术优点的入门知识。

我们特意将注意力放在技术细节上。这本书的主题是*计算机安全*（*computer security*），而不是笼统的信息安全。在这里没有涉及到诸如风险分析或是安全管理方面的问题，但是我们不应该有这样的误解，认为它们对于计算机安全不重要。相反，在没有考虑应用环境前，任何技术性的安全事项都没法确定。在上面提到的研究生课程里，那些讨论技术目标的课程是和一门关于安全管理的课程一起讲授的，这里的安全管理包含了和计算机安全相关的那些非技术的安全问题。即使在关注于技术问题，如果读者在读完这本书后，仍认为在系统的安全目标明确之前，提出“这个系统是安全的吗？”这样的问题是有意义的话，我会觉得自己很失败。

本书的内容是按照下面的框架来组织的。全书分成四部分，第一部分包含五章，接下来的三部分各包含四章。这四个部分是：

- **第一部分 基础知识**：在这部分中的材料是关于计算机安全两个方面的基础。在阐述计算机安全的基本概念的同时，也阐述了用在计算机系统核心的机制，这些机制为其他的安全机制提供了基础。
- **第二部分 实践**：介绍了操作系统的两个案例研究，Unix 和 Windows NT，以及所收集的已出现的错误，这些错误不应再重复；另外还有关于安全评估的概述。

- **第三部分 分布式系统**：包含了与计算机网络和 Web 安全性相关的典型问题的讨论；对于这样的环境，密码学是安全机制的基本源泉。这部分也可以称为“当前计算机安全的发展趋势”。
- **第四部分 理论**：这部分是围绕数据库安全来组织的，讨论了多级安全的问题。因为有了完善的理论，我们才能在一个虽然特殊但却明确的环境里阐述安全问题。

本书几乎每一章都可自成一本书。因此，由于章节的限制，必然只能讨论相关主题的某些部分。但愿这种一般性的讨论覆盖的内容仍然相当广泛，而且在本书中也包括了许多印刷的和电子的参考资料的出处。我已经决定提供一些包含有用材料的 Web 站点，但读者应该知道，我不能保证那些材料没有被移到别的地方去或是在读者试图访问时已经不再存在了。我希望我选取的那些站点是很稳定的，不会让读者太失望。

章节的排序反映了我在介绍计算机安全时的偏爱。这里有两个例子可以说明我这样选择是值得深入探讨的：

- 访问控制结构（第 3 章）放在安全模型之前（第 4 章）。这种方式的不足之处在于，它介绍了访问控制结构而没有给出策略，解释为什么某人会对访问控制使用一个特殊的概念。然而，我喜欢独立于任何特定的策略来讨论结构。在概念和特定的策略之间建立太强的联系可能会导致错误的结论，就像“我使用这种工具，所以我解决那个问题”一样。
- 分布式系统安全（第 10 章）放在密码学之前（第 12 章）。这种方式的不足之处在于，当介绍最初的安全协议时读者还没有获得密码学的背景知识。然而，我想鼓励学生去试着分析安全协议，而把密码算法看成黑匣子，只使用它们行为的抽象描述。

不同类型的课程都可以使用本书中的材料。更偏于实践的课程可以基于第 1 到第 14 章的内容，或许应跳过安全模型（第 4 章）和第 5 章中的特定系统的详细技术问题。当计算机安全和关于网络安全的课程一起教授时，第三部分的材料可以由第四部分的内容来代替。例如，如果学生已经有了并发控制的背景知识，那么第 16 章就很适合他们。特别侧重理论的课程可以忽略一些案例研究，把时间更多地放在第四部分上。

我已经努力使每一章都包括了练习题，但并不是说已经达到了在所有情况下都让我感到满意的程度。就我个人而言，我只能说计算机安全不是各种解决方案的一个简单收集，它不能简单地在经典的教科书的练习里得到说明。在有些方面，如口令安全或是密码学，很容易编写练习，这些练习已经有准确的答案，只要按照一系列正确的步骤就能得到。其他一些领域更适合采用课程设计、小论文或是讨论的形式。尽管用实际系统中的经验来充实关于计算机安全的课程是最自然不过的了，但在这本书中并没有包括实验教学的建议。操作系统、数据库管理系统或者“防火墙”是实践练习最基本的选择。实际的例子将取决于教师所能使用的特定系统。常常有很多关于特定系统的优秀书籍，介绍如何使用系统的安全机制。

因为这是一本教科书，有时我在练习里也包含了许多重要内容，这些材料在关于计算机安全的技术手册中也能找到。

我要感谢很多对这本书作出了贡献的人，同时我希望没有在此被提及的朋友不会生气。在伦敦大学的 Royal Holloway 有个信息安全小组，他们为我提供了给他们信息安全的理学硕士生（MSc）上课的机会。那些选我课的学生严谨地指出了我讲课材料中的各种错误和矛盾之处。Simon Foley、Heather Hinton、Cynthia Irvine、Li Gong、Ulrich Lang、Ralf Oppliger 和

Bart Preneel 审阅过我的手稿，尽力纠正我的错误概念，并且为这本书提供了很多有用的附加材料和参考资料的出处。我的工作单位，英国剑桥微软研究院，为我提供了必要的时间让我得以完成本书。

目 录

第一部分 基础知识

第二部分 实 践

第三部分 分布式系统