世界著名计算机教材精选

PEARSON

计算机安全导论

Michael T. Goodrich
Roberto Tamassia
著
葛秀慧 田浩 等 译

INTRODUCTION TO COMPUTER SECURITY

清华大学出版社

PEARSON

世界著名计算机教材精选

计算机安全导论

Michael T. Goodrich
Roberto Tamassia 著
葛秀慧 田 浩 等译

清华大学出版社
北 京

内 容 简 介

EISBN: 0321512944

北京市版权局著作权合同登记号 图字：01-2010-7570 号

图书在版编目（CIP）数据

计算机安全导论 /（美）古德里奇（Goodrich, M. T.），（美）塔玛萨（Tamassia, R.）著；葛秀慧等译.
—北京：清华大学出版社，2012.3
（世界著名计算机教材精选）
书名原文：Introduction to Computer Security
ISBN 978-7-302-27335-6

Ⅰ.①计… Ⅱ.①古… ②塔… ③葛… Ⅲ.①计算机安全－教材 Ⅳ.①TP309

中国版本图书馆 CIP 数据核字（2011）第 236980 号

责任编辑：龙啟铭
封面设计：傅瑞学
责任校对：李建庄
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
印 装 者：清华大学印刷厂
经 销：全国新华书店
开 本：185mm×260mm **印 张**：24.25 **字 数**：604 千字
版 次：2012 年 3 月第 1 版 **印 次**：2012 年 3 月第 1 次印刷
印 数：1～3000
定 价：49.00 元

产品编号：040263-01

译 者 序

当拿到这本书时，心中非常兴奋，自己一直想翻译计算机安全方向的图书。在翻译过程中，我抱着一种学习、学习、再学习的态度。每翻译完一章，我都会再次拜读原著。在此期间，我被作者广博的知识所吸引，感到写得非常棒。

这本计算机安全教材适用于计算机科学系列的导论课程。与其他的计算安全教材不同，它从计算安全应用的角度出发，无需计算机专业课的背景知识，用“刚好够用”的方法来引导学生进入计算机安全领域，通过本书，读者能学习到访问控制、防火墙和病毒等计算机安全等主题，还能学到算法、操作系统、网络、数据库和编程语言中的许多基本计算机科学的概念。通过本书，学生不但能了解计算机安全的基本概念，还将具备应对安全威胁及对策的工作知识。

在第1章，介绍了计算机安全的基础知识。第2章介绍了物理安全，其中涉及人们日常生活中的所遇到的锁、保险箱、智能卡和自动取款机等的相关安全知识。第3章从进程、内存、文件系统和应用程序的角度，全方位地介绍操作系统的安全。第4章专门介绍恶意软件及用户对其进行防御的对策。第5章按层展开网络中应该注意的安全问题，并介绍了针对不同攻击的防御措施。第6章介绍了应用层和DNS、防火墙、隧道、入侵检测和无线网络的安全。第7章介绍了Web安全，分别从客户端和服务器的角度出发，介绍了相关的攻击及防御策略。第8章介绍了加密，包括对称加密、公钥加密、加密散列、数字签名及AES和RSA。第9章介绍了安全模型与实践，介绍了了各种访问控制模型、安全标准、软件脆弱性评估、管理与测试、Kerberos身份验证及文件存储。第10章介绍了分布式应用程序的安全，主要涉及数据库的安全、电子邮件的安全、支付系统和拍卖、数字版权管理、社交网络和投票系统。

本书内容翔实、覆盖了计算机安全的方方面面，且深入浅出，是一本不可多得的计算机安全方向的入门书籍。它不仅有操作系统、数据库、网络等专业课程的基本概念，还使读者能具有必须的计算机安全常识，使用户在使用网上银行服务、购物和社交网络时，能清醒地认识到安全的重要性。

本书的习题也非常具有特色，细分为强化练习和创新练习和项目练习。强化练习测试读者对本章所介绍的主题和原则的理解程度，创新练习测试读者在新背景下应用本章所学知识的能力。在项目方面，有一个项目集，它既集中用于计算机安全的课程中，也用于涉及计算机安全主题的相关课程中。此外，还有各种的可选集能使教师定制项目，以适应不同的学习模式和实验室资源。

虽然在翻译过程中已经尽心尽力，但由于水平有限，难免会存在一些不足之处，希望各位专家学者给予批评指正。我会认真进行修正。另外，还有田浩、刘展威、张桂香、王顶、刘秋红、刘朝晖、焦仁普、朱书敏、盖俊飞、李超和郭立甫、张小蕊、段建勇、刘玲、李帅、程香萍、刘艳霞、黄丹雅、郑宏亮、刘丽华、杨希、晁静雅、赵倩、刘薇、张琳、

陈宗斌、陈红霞、张景友、易小丽、陈婷、管学岗、王新彦、金惠敏、张海峰、徐晔、戴锋、张德福、李振国、杜明宗、高玉琢、王涛、申川、孙玲、高德杰、宫飞、侯经国、刘淑妮、张春林、李大成、程明、张路红、张淑芝、孙先国、刘冀得、梁永翔、张广东、郁琪琳、邵长凯、蒲书箴、潘曙光、刘瑞东、李军、焦敬俭参加了本书的翻译，在此一并表示谢意。

我希望本书能够对想了解、学习和研究计算机安全的读者有所帮助，希望能够使计算机安全知识更加普及，每个人都能成为计算机安全策略的制定者和实践者。

译者

前　言

本书旨在从应用的观点来介绍计算机安全的一般原则。通过本书，读者能熟悉常见的网络攻击，包括病毒、蠕虫、密码破解、按键记录器、拒绝服务、DNS缓存中毒、端口扫描、欺骗和网络钓鱼。读者还能学到与计算机和网络脆弱性相关的鉴别和防御技术以及用于检测和修复受感染系统的方法。读者也将学习如加密、数字签名、加密协议和访问控制模型等安全系统的基本构建块。同时，读者还将学习如锁、手机、ATM机和信用卡等相关常用物品的安全原则。最后，读者将学习与人文、社会和经济相关的计算机安全，包括可用性、接口、数字版权管理、社会工程、垃圾邮件业务、伦理和法律问题。

方　法

本书的设计是独立的，而不是假设读者已掌握了操作系统、程序执行、网络、数据库和Web等的相关知识。在介绍相关主题的安全问题时，本书都介绍理解这些主题所必需的背景知识。因此，本书不同于高级课本，高级课本可能需要更广泛的计算机科学背景知识，并将重点集中在计算机安全方面。本书只需要计算方面的基本预备知识，所以它既适用于计算机科学专业的初级或中级学生，也适用于选修计算机科学专业的学生和非计算机科学专业的学生，当然假定后者略有计算机科学的背景知识。本书可以作为计算机安全导论课程的教材，它有助于提高学生的认知，并从计算机安全的视角获得计算主题的丰富知识。

此外，本书虽然讨论了加密，但它不同于纯粹的密码学教材，纯粹的密码学教材侧重于数学和安全的计算基础。而本书讨论加密时，先讨论加密所提供的功能和如何使用加密来建立安全的系统，稍后才涉及一些特定的加密方法。本书的最后三章对密码学进行了介绍，这部分是独立的，所以在计算机安全课程或自学时，读者可以根据需要，自行决定早点或晚点学习这三章内容。

先修科目

实践早已证明，计算机安全课程的教学是富有争议并具有挑战性的。第一个问题是这一课程所需的先修科目。传统上，计算机安全课程需要广泛的计算机科学和数学背景，且需要先修过如算法、操作系统、计算机网络或软件工程等初级/高级课程。典型的假设是，为了学习计算机安全，学生需要具备计算机系统如何运行的高级知识，且有非凡的编程能力和深厚的数学功底。这种方法为教师选择高级主题和项目提供了灵活性。但是，这也导致了精通计算机安全的信息技术专业人员的短缺。此外，这种传统方法也使选修计算机科学的学生和非计算机专业的学生不能学习计算机安全这门课程。

而这本计算机安全教材适用于计算机科学系列的导论课程，如作为原ACM计算机科学课程中传统的CS1/CS2系列。为了解决所需的背景知识，在介绍计算机安全时，为了使读者能理解所介绍的特定的计算机安全主题，本书同时提供计算所需的基础教程。因此，使用本教材的课程，教学能达到双重效果：既学习了如访问控制、防火墙和病毒等计算机安全主题，又介绍了在算法、操作系统、网络、数据库和编程语言中的许多基本计算机科学的概念。我们确信，本书能传授基本的计算机安全概念、能为学生提供刚好够用的应对安全威胁及对策的工作知识、也能为学生理解这些内容提供即时的计算机科学背景材料。因

此，在信息安全设置中，本书能运用和增加学生编程和算法的知识，因为对于开发有效的安全解决方案而言，坚实的编程训练和高效的算法都是至关重要的。

在先修课程方面：我们假设读者已熟悉某种高级编程语言，如C、C++、Python或Java语言，并能理解这类高级编程语言的主要结构。此外，我们还假设读者熟悉基本数据结构和计算机系统的基本概念。

计算机科学概念

本书是专为普及而写的，以便鼓励学生考虑安全问题，并在设计软件应用程序或决定购买计算机硬件或软件时，提前部署安全机制。这一技能的优势会在将来的就业中体现出来，在金融、医疗保健和技术部门的公司中，计算机系统的安全通常是至关重要的需求。除了训练信息安全技术的专业人才之外，本书的目标是培养具有计算机安全常识的用户，在网上银行服务、购物和社交网络等日常生活中，当用户使用计算机和互联网时，会对安全后果有清醒的认知。最后，但不限于此，最近电子投票以及广告客户和政府机构对互联网用户的跟踪也是编写本书的一个动机，我们希望学生能意识到对个人隐私存在潜在的威胁，且民主本身可能也存在问题，这些都源自于不当地使用计算机安全技术的缘故。

主题表格

本书的主题和相关的基本计算机科学概念如表1所示。

表 1 本书主题和相关的基本计算机科学的概念

主题	子主题	相关概念
代码执行	缓冲区溢出、沙盒和移动代码	编程语言、软件工程
恶意软件	病毒、蠕虫和检测	计算复杂性、模式匹配
访问控制	用户、角色、策略和文件权限	操作系统
验证	密码系统、散列、数字签名和证书	算法、数据结构和计算复杂性
网络安全	SYN 洪水、ARP 和 IP 欺骗、防火墙、拒绝服务和入侵检测	计算机网络的模型和协议
人类和社会问题	可用性、社会工程和数字版权管理	用户界面和计算机伦理学
Web 服务器	SQL 注入	数据库
电子邮件	垃圾邮件和垃圾邮件过滤	机器学习和计算复杂性

练习与项目

本书的每一章都包括大量的练习和项目集。练习细分为强化练习和创新练习。强化练习测试读者对本章所介绍的主题和原则的理解程度，创新练习测试读者在新背景下应用本章所学知识的能力。在项目方面，我们有一个项目集，它既集中用于计算机安全的课程中，也适用于涉及计算机安全主题的相关课程中。还有各种的可选集能使教师定制项目，以适应不同的学习模式和实验室资源。

致读者

对本书的读者而言，配套网站提供了以下的补充材料：

- 本书中选定习题的答案。
- 本书中大量主题的 PDF 格式的教案。
- 电子版的参考书目，可以链接到引用文章的授权电子版。

致教师

下面的补充材料有助于教师用本书来讲授这门课程：

- 包括本书大量主题的 PowerPoint 格式的教案。
- 选定习题的电子解决方案手册。
- 以下主题的完整的已开发的编程项目：
  （1）蠕虫的传播和检测。
  （2）防火墙的配置与管理。
  （3）Web应用程序和Web服务器攻击。
  （4）数字版权管理。

通过破坏安全或保护系统免受攻击的挑战，每个项目都能激发学生的创新能力。

关于作者

在计算机安全、算法和数据结构的研究中，Goodrich 和 Tamassia 教授是得到公认的，针对这些主题，他们已发表了多篇论文，并开发了计算机安全、密码学、云计算、信息可视化和几何计算的应用。在由美国国家科学基金会、美国陆军研究办公室和国防高级研究计划局资助的几个合作项目中，他们曾担任首席研究员。他们还活跃在教育技术研究的领域中，并已出版了若干书籍，其中包括被广泛采用的《数据结构与算法》这本教材。

Michael Goodrich在普渡大学获得计算机科学的博士学位。他目前是加州大学欧文分校计算机科学系校长级教授。此前，他曾是约翰霍普金斯大学的教授。他是*Journal of Computer and Systems Sciences*和*Journal of Graph Algorithms and Applications*的编辑。他是富布莱特的学者、计算机协会（ACM）的杰出科学家、美国科学促进会（AAAS）、ACM和电气和电子工程师学会（IEEE）的院士。

Roberto Tamassia在伊利诺伊大学香槟分校的电子与计算机工程系获得博士学位。他目前是计算机科学的Plastech教授，是布朗大学计算机科学系的系主任。他是*Journal of Graph Algorithms and Applications*的创刊人和主编。此前，他还担任了*Computational Geometry: Theory and Applications*和*IEEE Transactions on Computers*的编委。他是电气和电子工程师学会（IEEE）的院士。

除了他们的研究成果之外，作者还有丰富的教学经验。如Goodrich教过数据结构与算法课程、有作为初级课程的数据结构、有作为中级课程的应用密码学及作为高级课程的互联网算法。他还获得了许多教学奖励。Tamassia教过作为入门级课程的数据结构与算法、高级研究生课程的计算几何。在过去几年里，他已经针对大二学生开设了“计算机系统安全概论”这门新的计算机安全课程。 他从2006年开始讲授这门课程，这也有助于框定本书的主题。另外，他的教学风格与众不同之处在于：他有效地利用了与Web集成的交互式超媒体教案。

致谢

还有许多人对本书的编写做出了贡献。我们要特别感谢Dan Rosenberg，他深入地研究了一些主题，并给出了许多有用的建议，它们已成为本书大量的重要内容和插图。如果没有他，也不会有今天这本书。

Bernardo Palazzi渊博的知识和他在计算机安全的教学经验成了这本书写作的宝贵资源。我们感谢他给出专家意见和许多模拟讨论。

我们也感谢Wenliang Du的一些建议，感谢他所工作的美国国家科学基金会资助的安全

教育项目（SEED），它资助了本书中的几个项目。

我们感谢所有的研究合作者、助教和学生，他们促成了本书的完成，给出了有关章节早期草稿的反馈意见，并帮助我们编写练习、开发项目和提供补充材料。我们尤其要感谢Vesselin Arnaudov、Alex Heitzmann、Aaron Myers、Jonathan Natkins、Aurojit Panda、Charalampos Papamanthou、Neal Poole、Jennie Rogers、Michael Shim、Nikos Triandopoulos、Saurya Velagapudi和Danfeng Yao。

与几位同事的讨论也有助于我们强调本书的内容和格式。我们要特别感谢Mikhail Atallah、Tom Doeppner、Stanislaw Jarecki、Anna Lysyanskaya、John Savage、Robert Sloan、Dawn Song、Gene Tsudik、V. N.Venkatakrishnan、Giovanni Vigna和William Winsborough。

我们确要感谢外部评审者丰富的注释和建设性的批评意见，这些都是非常有用的。

我们感谢编辑Matt Goldstein，他给予了很好的支持并给出了完美的建议。Addison-Wesley团队已经非常了不起了。还要感谢Chelsea Bell、Jeffrey Holcomb和Jeri Warner。

本书的手稿主要是LATEX排版包。大多数的图是在Microsoft PowerPoint中绘制的。

最后，我们要衷心感谢Isabel Cruz、Karen Goodrich、Giuseppe Di Battista、Franco Preparata、Ioannis Tollis和我们的父母在本书编写的各个阶段所提供的意见、鼓励和支持。我们也感谢在写书之外他们对我们生活的照顾。

Michael T. Goodrich

Roberto Tamassia

目　录

第1章 简 介

1.1 基本概念

我们将在本章介绍计算机安全的一些基本概念。主题从理论密码学原语（如数字签名）到实际的可用性问题（如社会工程）。这一章给出了各种主题非正式的直观描述，在本书的后续章节中将更详细地介绍这些主题。

现有的计算机系统可能包含早期版本的旧功能，这些功能可以追溯到很久远的时代，如互联网只用于学术研究人员和军事实验室的时代。举例来说，网络连接的计算机之间相互信任且没有恶意行为的假设在20世纪80年代初可能是合理的，但现在这种假设在互联网操作中仍然存在，这是非常令人惊讶的。这种假设已经导致基于互联网犯罪的增长。

计算机安全的一个重要方面是计算机系统的**脆弱性**（vulnerability）识别，举个例子，利用脆弱性，恶意用户可以访问私有数据，甚至可以完全控制计算机。针对脆弱性会产生各种**攻击**（attack）。通过分析这些攻击，可以确定攻击所能造成破坏的严重性以及该攻击被进一步复制的可能性。为了防御攻击，需要采取的防护措施包括识别目标计算机、删除恶意代码和为系统打补丁来消除脆弱性。

为了建立安全的计算机系统，首先要有合理的**模型**（model）。特别是，定义必须保证的**安全属性**（security property）、预见可能发动的攻击类型以及制定具体的防御都是非常重要的。**设计**（design）也应考虑可用性问题。事实上，安全措施不但难于理解，而且使用麻烦，那么采用这样的安全措施极有可能会导致失败。其次，为了检测引入脆弱性的编程错误，要严格测试系统的硬件和软件实现（implementation）。一旦部署了系统，相关程序应该到位，以**监测**（monitor）系统的行为、发现安全隐患并做出反应。最后，系统一旦变得可用，就必须先应用与安全相关的**补丁**（patches）。

在更广泛的上下文中，通过分析问题，经常能更好地理解计算机安全的概念。出于这一原因，本书还包括了各种真实的、现实世界系统的讨论，包括锁、ATM机和机场的旅客安检。

1.1.1 机密性、完整性和可用性

计算机和网络被滥用的速度正在增长。垃圾邮件、网络钓鱼和计算机病毒已造成数十亿美元的问题，因为是身份盗窃，所以对个人财务和用户的信用等级构成了严重威胁，并造成了企业的负债。因此，与信息技术专业人员需要增长专业知识一样，在社会中，人们对更广泛的计算机安全知识的需求正在日益增长。社会需要受过更多的安全教育的计算机专业人员，他们能成功地防御和避免针对计算机的攻击，同样也需要受过安全教育的计算