美国最畅销“傻瓜”丛书

COMPUTER SECURITY FOR DUMMIES

“傻瓜”系列

计算机安全保密指南

[美] Peter T. Davis
Barry D. Lewis 著

薛荣华 章晓莉 赵继红 等译

王仲文 薛荣华 审校

- 保护计算机免遭黑客、病毒及其他意外事故攻击的简单易行办法——全新的！
- 帮助你识别系统探查、口令被窃等计算机威胁的工具软件包
- 简单明了地解释安全措施的实施

IDG BOOKS WORLDWIDE

PHEI

电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

包含如何保持E-Mail秘密的建议！

美国最畅销“傻瓜”丛书

计算机安全保密指南

[美] Peter T. Davis & Barry D. Lewis 著

薛荣华 章晓莉 赵继红 等译
王仲文 薛荣华 审校

電子工業出版社

内 容 简 介

当今世界，计算机不仅是计算机专业人员而且也是普通百姓的重要工具。人们用计算机处理许多重要的信息，因此计算机的安全保密性也变得愈来愈重要。本书将帮助你解决如何保护有价值的数据及系统资源问题。首先解释计算机有哪些安全问题，然后提供一些有效的技术来进行保护，本书分为独立的五个部分，第一部分是计算机安全的基本知识，讨论安全的目标——机密性、完整性及可用性，介绍威胁、风险、脆弱性及控制等安全术语、以及如何进行风险分析以确定风险等级及需要的安全措施。第二部分讨论一些保持计算机安全的方法，包括物理安全措施、对计算机的访问控制、如何使用内部的安全特性、口令、备份及数据恢复。第三部分揭露一些有安全性问题的场合。在使用 Internet 和联机服务发 E-mail 及文件时如何防止窥探者阅读你的文件及用加密的方法保护你电子邮件的秘密。第四部分是十准则集粹，内容包括十种最流行的病毒、十种最有用的备份设备、以及保护 DOS、Windows 及 Macintosh 计算机系统的方法等。第五部分是附录，收集了读者需要的重要信息，如讨论计算机安全的出版物和 Internet 场部、安全软件和产品的来源、计算机安全术语及缩略语等。

读者对象：计算机爱好者、管理人员及广大计算机用户。

美国最畅销《傻瓜》丛书

计算机安全保密指南

薛荣华 章晓莉 赵继红 等译

王仲文 薛荣华 审校

责任编辑：洋溢

电子工业出版社出版（北京市万寿路）

电子工业出版社总发行 各地新华书店经售

北京市顺义县天竺颖华印刷厂印刷

开本：787 × 1092 毫米 1/16 印张：17.75 字数：432 千字

1997 年 3 月第一版 1997 年 3 月第一次印刷

印数：8000 册 定价：30.00 元

ISBN 7-5053-3880-3/TP·1669

著作权合同登记号 图字：01-96-1004 号

作者简介

Peter T. Davis

Peter 是一家专门从事信息系统安全、审计及控制的管理咨询公司 Peter Davis +Associates 公司的奠基人和负责人。他曾在计算机安全协会及信息系统安全协会的部门工作过。此外，他是为开发一般可接受的系统安全准则(Generally Accepted System Security Priciples，GSSP)、一种国际安全方法学而成立的委员会的成员。Peter 已编著、合著或编辑过四本别的书。

Barry D. Lewis

Barry Lewis 在 1969 年开始地的计算机生涯，为一家主要的金融机构工作并延续了近 18 年。他的第一台个人计算机拿今天的标准看，功能比廉价的计算器还差。1980 年当他参加开发银行的安全程序时，他开始探索计算机安全。从那时起便陷入这一领域。

1987 年他从金融领域转移到咨询业，参加了一家世界上最大的审计公司。不久，他参加了第二大国际审计公司，为北美的组织机构提供安全咨询达五年之久。1992 年他进入保密实践领域，并在 1993 年参加了一家叫作 Cerberus Information Security Consulting Inc. 的小咨询公司。你可以在 www. cerberus. com /～cerberus 上找到他们的 Web 页。

Barry 在北美给各种各样的组织机构开办培训班，包括计算机安全协会(CSI)、计算机企业安全与审计年会(ESAC)及 EDPAA。1994 年，在 ESAC(北美的一次最大的安全会议)上获最佳发言奖。

Barry 是一位多产作家，在 Auerbach、Computing Canada 及 Journal of Systems Management 等杂志上发表多篇文章。他是 1996 年春出版的《客户机 /服务器安全》一书的合著者。

译者序

第一台电子计算机诞生至今已整整五十年了，这一高科技产品经过数十年的发展，已经演变成信息社会的基础，不但政府机关、企事业单位、院校和科研机构、生产和管理部门大量使用、构成庞大的信息网络并实现了信息共享，而且已经进入寻常百姓家庭，成为每个人不可缺少的信息工具。随着计算机的大量使用，计算机的安全问题也愈来愈突出，计算机病毒、计算机犯罪以及计算机所面临的各种风险正威胁着计算机及计算机网络发挥其巨大的威力。据今年 4 月 30 日至 5 月 2 日于伦敦举行的英国“1996 年信息安全博览会”公布，英国去年因计算机犯罪损失达 15 亿美元，全球去年因计算机损失 150 亿美元。预计到 2000 年，这一数字将高达 2000 亿美元。面对这个惊人的统计数字，广大的计算机用户能无动于衷吗？那么，怎样才能采取必要的防范措施，确保安全地使用计算机、免遭不必要的损失呢？这就是本书作者要向广大计算机用户介绍的主要内容。

本书以通俗易懂的语言向读者介绍了计算机安全领域的基本知识、使计算机安全的各种方法、要注意计算机安全的场合，并以十点集粹的形式介绍了各种计算机安全产品，在附录中还收集了与计算机安全有关的重要资料以及名词解释和缩略词等。相信广大读者读了这本书后会对计算机安全有一个新的认识，并从中汲取有效的防护措施来改善你计算机的安全水平。

本书由薛荣华（第三、四、五部分）、章晓莉（第二部分）、赵继红（第一部分）翻译，由王仲文（第三至五部分）、薛荣华（第一、二部分）审校。对本书译、录、校工作给予大力协助的还有闫慧娟、徐宏、陈建平 、邓波、薛菲、雪山、许新华、严光泽、徐亮、童刚、张力等同志。《今日电子》杂志社的编辑们为本书的出版作了大量艰苦细致的工作。译者谨向他们表示衷心的谢意。由于译者水平有限，中译本中疏漏不妥之处在所难免，欢迎广大读者批评指正，谢谢！

译　者

1996 年 8 月

目　录

前 言

* *

当今不断变化着的现代社会里，计算机不仅是计算机专业技术人员，而且也是普通人的有用工具。今天的计算机能处理一切事务，从你家庭的流水帐、孩子的家庭作业、直至祖母的菜谱。因为我们知道，这些信息对你是重要的，我们想帮助你熟悉计算机安全的概念。

本书能帮助你——普通的非计算机专业人士——计划和实现计算机安全的各个方面，理解备份系统及使数据安全的必要性。这样，即使硬件或软件出现故障，你仍可以恢复数据。或者，如果有人想要得到你的个人数据，该闯入者得不到访问权、或只能读到不可懂的垃圾式数据。

关于本书

《计算机安全保密指南》帮你弄清楚怎样保护有价值的数据与系统资源，本书有两个目的：首先，我们解说安全问题；其次，向你提供一些保护技术。利用这本书，你会明白下列事情该怎样做：

√ 鉴别对你的系统和数据的威胁。
√ 认识与那些威胁有关的风险。
√ 控制你的环境。
√ 避免常发生的错误，如在系统上溅饮料或遭遇电源故障。
√ 在 Internet 及其他商业联机服务上找有用的资料。
√ 购买安全硬件和软件。

读者对象

写本书时，我们认为你是：

√ 肯定不是傻瓜、或不关心 PC 机安全的人。
√ 对防止你的数据及系统免遭意外的或故意的伤害感兴趣。
√ 使用一台运行 Apple 的 Mac OS 或 Microsoft 的 Windows 的 PC 机。
√ 不想成为安全专家，但想听实际忠告。
√ 有兴趣继续使用你的计算机娱乐或赚钱。

本书的结构

本书分为五个部分。你不必依次阅读，但这样做有好处。虽然你可从任意处开始并只读你感兴趣的部分，但请你至少浏览一下第一部分以便熟悉那些必要的安全术语。

第一部分：安全的基本概念

第一部分是理解安全的基本知识。你会读到安全的目标——保密性、完整性和可用性。此外，我们向你介绍威胁、风险、脆弱性及控制。这一部分中的材料包括众所周知的威胁讨论及预访、发现和更正的控制。你熟悉了这些术语后，可以将它用于你的环境中。这一部分还向你说明如何完成风险分析，以确定你的风险级别。

第二部分：安全的方法

理解了各种威胁及脆弱性之后，你就可以选择并实现专门的补救控制措施。读一下第二部分中的获得访问控制权、挑选好的口令、利用内部的安全特性、进行备份及恢复数据。

第三部分：不安全的场合

第三部分揭露一些你可能会暴露的场合。因为许多人正连接在联机服务上并使用电子邮件，我们告诉你，使你的 e-mail 安全、加密、滤除、真正的文件擦除、访问控制及复制等问题。

第四部分：十准则集粹

正如该名称所隐喻的，第五部分向你提供我们在写本书时收集的有价值的东西。这一部分支持其他章节，例如，我们谈论过病毒，但在这一部分里，我们介绍十种蔓延最广的病毒。你还可以发现备份你系统的办法及保护 DOS、Windows 及 Macintosh 计算机的方法。

第五部分：附录：参考资料

附录 A 中，我们介绍有用的安全硬件及软件的提供者，以及与安全有关的组织机构，还提供书籍和期刊一类的出版物的名称。

附录 B 告诉你到哪里去联机查找计算机安全的资源。

附录 C 名词解释定义了所有的安全术语。每个专业和准专业都有那些只有内