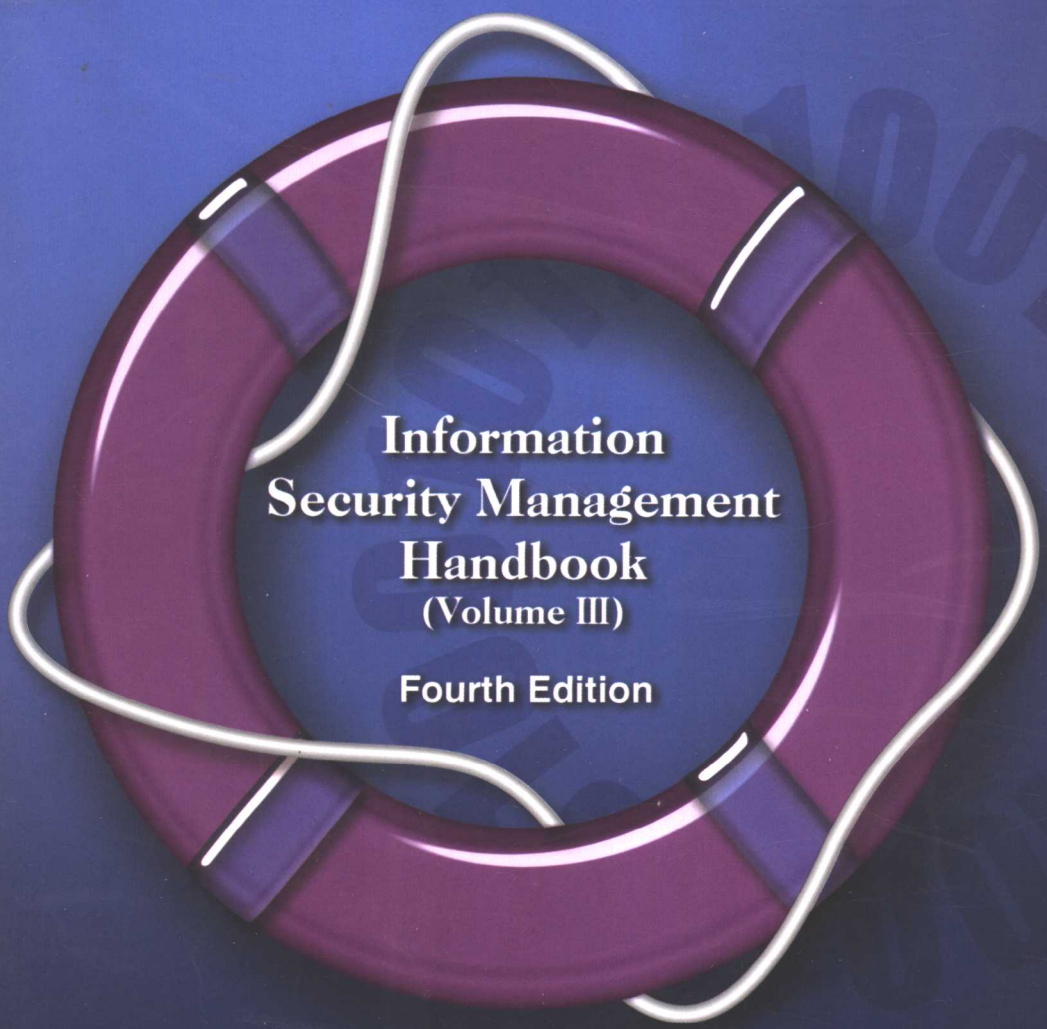

Information Security Management Handbook (Volume III)

Fourth Edition

信息安全管理手册（卷III）（第四版）

[美] Harold F. Tipton Micki Krause 主编
张 文 邓芳玲 程向莉 吴 娟 译

AUERBACH
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

电子信息科技专著出版专项资金资助出版

信息安全管理手册（卷Ⅲ）

（第四版）

Information Security Management Handbook(Volume3)

Fourth Edition

[美] Harold F. Tipton Micki Krause 主编

张 文 邓芳玲 程向莉 吴 娟 译

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

随着科学技术的迅猛发展，信息安全人员面临着越来越大的挑战。本书汇集了各种技术的最新发展趋势、新概念以及相应的安全管理方法，系统、全面地阐述了与信息安全管理相关的内容。全书分为 10 部分，内容包括：访问控制系统和方法，电信和网络安全，安全管理实践，应用程序和系统开发的安全性，密码术，安全结构和模型，操作安全，商业持续性计划和灾难恢复计划，法律、调查和道德标准，以及物理安全。

本书既适合作为参加 CISSP 证书考试的教材，又适合信息安全技术人员和管理人员用做日常参考手册。

版权贸易合同登记号　图字：01-2002-5473

图书在版编目(CIP)数据

信息安全管理手册. 3 卷：第 4 版/（美）泰普顿（Tipton, H.F.），（美）克劳斯（Krause, M.）著；张文，邓芳玲，程向莉译. —北京：电子工业出版社，2004. 6

书名原文：Information Security Management Hand book

ISBN 7-5053-00044-6

Ⅰ. 信…　Ⅱ. ①泰…②克…③张…④邓…⑤程…　Ⅲ. 信息系统—安全管理—技术手册　Ⅳ.TP309-62

中国版本图书馆 CIP 数据核字（2004）第 046361 号

责任编辑：张来盛
印　　刷：北京民族印刷厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：28.5　字数：728 千字
印　　次：2004 年 6 月第 1 次印刷
印　　数：5 000 册　　定价：52.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译 者 序

网络信息安全在国家信息化建设过程中占据非常重要的地位，经过十多年的飞速发展，网络已成为我国与世界进行信息交流的主要手段。网络上信息资源的安全性就显得格外重要，尤其对一些相当重要的数据、资料的安全保护已成为网络安全管理的必然趋势。网络的快速发展是国家信息化发展的前提，而信息安全管理已成为当前网络发展的主要切入点。因此，采用何种保护手段、运用哪些保护措施以及应该保护哪些内容，成为网络安全管理的主要研究内容。

网络信息安全是一项动态的、整体的系统工程，从技术上来说，网络信息安全由安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成，一个单独的组件是无法确保信息网络的安全性的。

本书重点针对一些普遍性问题和所应采用的相应安全技术，系统、全面地介绍了信息安全管理的相关技术、设备、应用和防范措施。本书具有以下显著特点：

（1）权威经典。本书原作者是美国长期从事网络安全研究、设计和标准制定的知名专家，已有多部关于网络安全的专著出版。其内容构成了系统的理论体系，在学术上具有国际领先水平，又涵盖了最新的网络安全技术，具有相当的权威性。

（2）全面、系统。本书篇幅较大，覆盖面广，内容涵盖了网络技术的方方面面和相关的标准，是目前信息安全管理类书籍中“最全面、最系统的一本技术专业书籍”。

（3）技术先进，具有现实性和前瞻性。本书密切结合实践，注重技术的先进性，对当今网络发展中的新技术和新应用，如生物测量学、远程通信和网络安全、ERP 的安全、注册信息表的安全、物理层的安全、网络层的安全、安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等，都进行了系统阐述。

（4）内容新颖，具有独创性。本书循序渐进，深入浅出，层次清楚，详简得当，按照不同研究领域分开叙述，从一般到特殊、由基本到全面进行讲述。各篇相互独立，自成体系，以满足不同的读者需求。

（5）理论与实践紧密结合。本书既有丰富的基本理论，又汇集了多年来网络安全发展的最新经验，对于网络安全管理的工程设计、系统维护等实践都具有重要的指导作用和较高的应用价值。

（6）实例、资料丰富。本书提供了大量的实例和技术资料，可使读者举一反三，推广、应用到具体工程实践中去。

本书概括了目前美国 IT 业界对网络安全管理的建设经验，从网络安全的保护手段、保护措施、保护的内容出发进行详尽的分析，对提高现有网络质量，确保网络安全，开展新业务，以及帮助领导决策都将起到新的作用。

本书主要由张文、邓芳玲、程向莉、吴娟翻译，参加翻译的还有邢淑琴、杨弃、吴春清、卢醒春、陈春生、俞海莹、汤志强、张明安等，在本书翻译过程中，邵自力研究员、吴吉祥研究员给予了亲切指导。在此表示感谢。

由于译者水平有限，不妥之处在所难免，恳请读者指正。

前　言

信息技术的迅猛发展，使信息安全专业人员面临着越来越大的挑战。因此，我们很高兴将《信息安全管理手册》（第四版）的第3卷奉献给广大读者，其中讲述了不断发展的技术的形成趋势、新概念以及安全方法，旨在为信息安全人员提供最新内容的日常参考手册——这也是我们不变的承诺。

再者，我们根据信息安全知识共同体（CBK）的要求不断调整《信息安全管理手册》的内容，以便为信息安全专业人员准备CISSP证书考试提供参考资料。CISSP证书考试和CBK研究班课程由国际信息系统安全证书联盟（$(ISC)^2$）举办，世界各地都在开展，而且具有很大的需求。

准备CISSP证书考试需要付出巨大的努力，这是因为它要求全面理解和应用CBK中所包含的主题。《信息安全管理手册》系列图书被认为是准备CISSP证书考试的应试者使用的一种最重要的参考书。技术人员在日常工作中也使用这些图书，他们经常要用到书中所提供的实践信息。

面对计算机病毒和蠕虫的不断增殖，以及恶意黑客利用开放网络协议的安全漏洞而发起的威胁，勤勉的首席执行官（CEO）们（他们有责任保护公司的资产）不得不聘用最高素质的安全职员。因此，同以前相比，如今在招聘时更要求有CISSP指定证书。

这一版《信息安全管理手册》及其将来版本，特意将内容按照CISSP证书考试的各部分进行编排。每本书都有一章或几章讲述宽范围的信息安全领域中所包含的特定CBK主题。因此，我们的目的是保持在每一版中都有一些全新的章节，以确保书中的内容随着信息安全领域的技术发展而保持同步。同以前的版本相比，这一版任何一章内容都不重复。

Harold F. Tipton
Micki Krause

目　录

第 1 部分　访问控制系统和方法

第 2 部分　电信和网络安全

第 3 部分 安全管理实践

第 4 部分 应用程序及系统开发的安全性

第5部分 密 码 术

第6部分 安全结构和模型

第7部分 操 作 安 全

第 8 部分　商业持续性计划和灾难恢复计划

第 9 部分 法律、调查和道德标准

第 10 部分 物 理 安 全

第 1 部分　访问控制系统和方法

倘若认识到信息是无价的而且必须保证信息不被误用、泄露和破坏，很多机构就会实施访问控制，以确保那些用以做出关键商业决定的信息的完整性和安全性。可以采用很多方法控制对计算资源和信息的访问。但是，不管采用什么方法（无论是技术方法还是管理方法），访问控制对一个完善的信息安全系统来说是非常重要的。

这部分讲述用户身份识别和验证，访问控制技术及其管理，以及攻击方法的演变和改进。

生物测量学（生物统计学）用来进行个人身份识别和验证，由于它具有根据一个人的个性特征（如声音、手印、指纹和视网膜图等）准确地识别这个人的能力，因而正迅速成为访问控制的通用方法。虽然生物测量设备已问世多年，但新的方法不断出现。了解了这些重要工具的潜力和局限性，就能合理而有效地应用这些技术。

访问控制的使用没有保护病人健康资料的保密性和安全性重要。在北美之外，特别是欧洲国家，多年来隐私已成为重点。最近美国的消费者要求保护他们的个人隐私，有证据表明他们的医疗信息正成为被泄露的对象。1996 年的 HIPAA 法案（健康保险携带与责任法案）和 1999 年的 Gramm-Leach-Bliley（GLB）法案，证明美国政府正注意到民众的要求。

恶意的攻击正不断地破坏信息控制和降低信息安全性。黑客试图突破一个机构的防卫，而且大多数情况下都获得成功。在本部分中，读者将了解很多先进的现代化攻击工具，这些工具已导致一些广为人知的案例。例如，最近美国司法部的网站被破坏，很多商业网站受到拒绝服务攻击。

社交工程技术是一种利用人的天性很容易就对系统进行控制的方法。在社交工程中，一些无赖采用不正当的办法获得可以用来进行攻击的信息。例如，假扮技术人员给不设防的用户打电话，说需要该用户的网络口令来诊断一个技术问题，然后用该口令来破坏系统。

第 1 章　生物测量学：有哪些新技术

多年来，网络世界的安全建立在口令、个人身份号（PIN）或自己母亲名字之类个人信息基础上。现在可以把生物信息作为补充。生物测量学（生物统计学）从手指、眼睛和面部特征等方面测量一个人，还包括他如何说话和走路的方式等；不久还可以根据一个人的耳朵构成方式以及他如何听取声音来进行测量。

以下简单介绍传统的生物测量学系统以及新的技术和系统。

1.1　指纹

几年之后，用黑墨水获得指纹的方法将过时。人类将进入指尖传感器时代，用指尖触摸传感器可以快速访问远程网络。用户不必担心指纹被仿造，因为没有两个指纹是完全相同的。

指纹由一些纹路组成，包括断点和分岔，就是所说的指纹索引的细节。一个指纹平均有40～60 个细节。但即使一个指纹模型有足够的细节数，传感器还是有可能无法捕捉所有的细节。对某些人而言，因为每天敲击键盘或弹钢琴，使他们的指纹模型变得很细。另外，如果一个人手指有天生的缺陷或者有疤痕，则他们的指纹模型很难识别。

将指纹模型和登记的指纹对照的方法有 4 种：电子式、热敏式、光学式和混合式传感器。电子式传感器测量指纹高低电场强度。热敏式传感器测量手指接触时指纹凹凸部位的温度差。光学式传感器测量指纹的波长差。混合式传感器是光学式和电子式捕捉设备的结合。

1.2　眼睛扫描

眼睛可以提供几千个细节。指纹细节提供的是外置结构的模型，而眼睛细节提供的是内部结构的模型。可以从两个来源获得这个信息：视网膜和虹膜扫描系统。前者关注视网膜静脉的模型，后者采用虹膜内纤维、组织的模型。

为获得视网膜独特的模型，视网膜扫描仪使用低强度光源，它要求被扫描者往里看并聚焦在一个特定点上。这样对那些戴校正眼镜和不习惯近距离接触者引起不便。

至于虹膜扫描，它使用传统的电视照相设备，无须近距离接触。在光线良好时，这对戴校正眼镜和适当距离接触都工作得很好。一些航线上安装了虹膜扫描仪，以加快旅客登机的过程。

要记住，眼睛模型可能会因为疾病或受伤而发生变化。眼睛扫描仪对盲人和那些视力受损者（尤其是视网膜受损的人）无效。

1.3　面部识别

面部识别系统可以在人出现在电视或闭路摄像头前时自动扫描人的面部。一种新系统工作在暗处，获得面部的热红外模型。赌场已在面部扫描方面投资建立面部数据库，以便保安快速识别作弊高手。