IT先锋系列丛书

无线安全

——模型、威胁和解决方案

WIRELESS SECURITY

MODELS, THREATS, AND SOLUTIONS

Randall K. Nichols
Panos C. Lekkas 著

姚 兰 惠俊红
郑家玲 张鸿燕 译
刘景伟

王新梅 姚 兰 审校

Mc Graw Hill Education

人民邮电出版社
POSTS & TELECOM PRESS

IT 先锋系列丛书

无线安全

——模型、威胁和解决方案

Randall K. Nichols Panos C. Lekkas 著

姚 兰 惠俊红 郑家玲 张鸿燕 刘景伟 译

王新梅 姚 兰 审校

人民邮电出版社

图书在版编目（CIP）数据

无线安全：模型、威胁和解决方案/（美）尼克尔斯（Nichols,R.K.），（希）莱卡斯（Lekkas,P.C.）著；姚兰等译.
—北京：人民邮电出版社，2004.11
（IT 先锋系列丛书）
ISBN 7-115-12860-X

Ⅰ. 无… Ⅱ. ①尼…②莱…③姚… Ⅲ. 无线电通信—安全技术 Ⅳ. TN92

中国版本图书馆 CIP 数据核字（2004）第 116131 号

IT 先锋系列丛书

无线安全——模型、威胁和解决方案

◆ 著 Randall K.Nichols Panos C.Lekkas
译 姚 兰 惠俊红 郑家玲 张鸿燕 刘景伟
审 校 王新梅 姚 兰
责任编辑 李 健

◆ 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 010-67129258
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：800×1000 1/16
印张：30
字数：658 千字 2004 年 11 月第 1 版
印数：1-3 500 册 2004 年 11 月北京第 1 次印刷

著作权合同登记 图字：01-2001-4496 号

ISBN 7-115-12860-X/TN・2369

定价：49.00 元

Randall K. Nichols&Panos C. Lekkas

Optical Switching and Networking Handbook

ISBN: 0-07-138038-8

北京市版权局著作权合同登记号：图字：01-2004-3157

内 容 提 要

伴随着无线技术特别是未来的 3G 技术在我们生活中的广泛应用，无线技术的信息保护已经迅速成为今天科技创新者们所面临的最重要并且最富争议的挑战之一。本书以一种可读性很强而且有效的方式，对无线技术发展中所关注的安全问题提出了具有深刻洞察力的见解。本书的目标是探索无线科技、技术和方法这一宽广的领域；提供有关的分析和见解；增进对安全的理解并延长应用的寿命。

本书所面向的对象是管理者、决策者、设计人员和项目主管。它有利于这些人尽职地保护其所在机构至关重要的无线信息资产和系统。本书也适合于无线计算机安全专业的一年级研究生课程，以及工程/MBA 项目。

序

无线技术方面的信息保护，已经迅速成为了今天科技创新者们所面临的最重要并且最富争议的挑战之一。随着融合了因特网技术的第三代（3G）移动通信，（一种通过无线网络和光纤网络，将移动设备连接到因特网并允许用户接收和发送详细信息的能力）技术的出现，为保护这些无线网络中的重要数据所必需的安全措施，已经变得更加难懂和复杂。在联网的无线设备中，围绕“适度安全”的有关争论在个人、商业和政府利益之间的竞争中存在已久。虽然保护个人隐私极为重要，但也有许多人主张个人隐私必须与一些利害关系相平衡，比如公众安全以及执法部门监视嫌疑犯私人通信的能力。此外，提供适当的安全措施，其相关的商业成本往往很高。

由于私人的和公共的信息基础设施部门的合并，使得现在的安全难题更加阴云密布。以前由独立的控制措施所管理的领域，现在通过公共交换网（Public Switched Network，PSN）这一通用手段来交换信息和工作。无线技术已经发展到了能够传送越来越大量的有价值信息，这就需要更高的保密性和安全级别。有人把 PSN 称为电信的“州际高速公路”系统，然而，无线正日益充当着这个巨大的全球信息基础设施的“下滑坡道”。

根据我的工作经验，我认为侦听无线通信是成功实现情报活动的关键。在第二次世界大战期间就是如此，整个冷战期间也是，今天仍然如此。在基于计算机的数字网络使用之前，无线通信形式的数据只有在传输期间容易受到攻击。因此只有在传输的那一刻才可能收集到情报，否则机会就错过了。情报人员学会依靠来自无线系统的通信情报，作为提供无价的战略和战术情报的一种手段。经验告诉我们，必须在战术信息甚至更重要的战略信息在被传送时的精确时刻，保护通信的安全。近年来发生的局部战争，进一步说明了无线通信如何能转化成立即生效的情报，这样的情报是难以从任何其他来源获得的。今天，关系到数据在线生成、传输和储存的庞大网络，使得相互联网的国家成了全世界最容易受到信息攻击的目标。这些安全脆弱性包括：以情报为目的的信息捕获，破坏或窜改信息，或者销毁网上数据。因为联网能力增加了生产力和效率，创造了财富，它传送着大量至关重要的信息，所以这些联网国家可能受到的损失要远远大于不如他们那么发达的国家所受到的损失。举例来说，恐怖分子可能会瞄准货币系统、一个转移和记录金融交易的联网的基础设施，这种类型的财富绝大多数都是储存在数据库中，容易被老练顽固的对手破坏。

当我们延伸和提高网络的连通性时，我们受到恶意攻击的弱点只会增加。军事优势不能完全提供我们过去已经习惯的那种保护。恐怖分子和其他攻击者有能力获得破坏性极大的网络武器，而且他们实行破坏的手段也增多了。正如最近 Hart Rudman 在关于 21 世纪国家安全的报告中所作的预计，如果没有采取足够的保护措施，在美国将会发生灾难性事件。因为新的数字网络信息技术，我们的边防将会出现更多漏洞；一些漏洞将会被消除还有一些会被攻

破。美国情报局将会面对更具挑战性的敌手，即使是最好的情报防护措施也不能防止所有意外的发生。依赖未加保护的网络，随之而来的风险是政府服务的损失、军事失败、以及灾难性的经济后果。

美国军方越来越依赖专用信息基础设施来实施其必要的军事行动。风俗习惯、文化和法令使得这种依赖更加复杂，法令使美国军方将焦点集中在国外军事行动上，并且限制国境以内的任何阻止或牵制不对称攻击的企图。将来，美国公民、军队和保密部门之间的合作和协调会变得十分必要。必要时，数据必须共享，以便迅速综合成有用信息，供军事行动决策人参考。同样地，政府提供的信息也必须流入保密部门以保证正确的认识和决策。

对于一个靠网络运转的社会，不断增强的移动性已经成为关键的益处。随着移动技术和设备的不断发展，运营商干劲十足地行动起来，通过移动的道路来扩展有线网络。对此，企业和服务供应商有把握能够办到。对于移动无线用户而言，价值在于远距离通信的能力；而在实践中，成本也必须相对适度。由于我们如此多的国家财富都依靠利用无线设备作为输入和输出的网络，显然需要更加关注必需的安全措施建设。此外，在整个因特网用户群体中需要形成一种新的安全文化。我们必须抵制对黑客伦理的美化，即所谓“破坏源于好奇”的说法。我们需要发展一种文化，强调每个因特网使用者——从学生到CEO——身负的责任和义务。正确的在线安全习惯必须成为人们的第二天性，以保护隐私和更广泛的社会利益。这包括所有显而易见的、我们应该做却往往没做的事：变换口令，不上网时断开连接，每天运行防病毒软件，每次购买新设备时都要改掉缺省密码，使用适当的安全和加密服务。除了个人行为之外，公司也必须了解并采取适当的安全技术以保护今后的安全。无线工作环境更需要发展这种新的安全文化。

《无线安全》一书以一种可读性很强而且有效的方式，对发展中所关注的安全问题提出了具有深刻洞察力的见解。作者广博的实践和学术背景，使他们能够通俗地介绍与无线安全相关的信息保护和安全脆弱性的最新情况。本书论述形式有条不紊，易于理解，并且引用文献充分。书中所列举的案例真实切题，与主题的中心思想紧密相关。作者在书中告诉读者危险所在，研究了一些人和系统沦为牺牲品的案例，并给那些由于这些安全风险而受害的人提供补救措施。

读者将会发现作者采取了很好的模式来安排他们的素材——一个技术认证结合一个解决无线通信安全问题的系统方法。本书针对的读者是工作在行政、决策或管理层的人员，以及那些有责任保护其机构的信息资产、知识产权和通信系统的人员。本书内容对于保密部门和政府管理人员也同样具有参考价值。

如何花费紧缺的资源才能实现一个无线安全问题的平衡的、多学科解决方案？关于这个问题，《无线安全》一书提供了一个利于正确决策的合理方法。最终的结果是，要有一个必要、可行的安全响应组织和政府机构或者类似的部门。

J. M.（Mike）McConnell，美国退役海军中将
Booz • Allen & Hamilton有限公司副总裁
国家安全局（NSA）前局长（1992～1996）

关于 J.M.(Mike) McConnell

作为 Booz • Allen and Hamilton 有限公司的副总裁，McConnell 先生负责为美国联邦政府的部和局以及商业客户提供信息保证。此外，他还指导公司为美国国防部进行信息业务。从 1992 年到 1996 年，McConnell 先生担任美国国家安全局（NSA）局长，该局负责信息情报以及用于保护政府机密信息的所有安全服务。他还在前苏联解体期间和沙漠风暴军事行动中担任过美国参谋长联席会议主席的情报官员。

在 Booz • Allen and Hamilton 公司时，McConnell 先生受总统委托负责关键基础设施保护，重点集中在银行和金融业的安全标准上。他还在美国白宫的关键基础设施保证办公室（CIAO）任职，他领导的小组制定了美国国家基础设施保证计划的设计和计划方针。McConnell 先生还帮助司法部/联邦调查局开发了新的国家基础设施保护中心（NIPC）运作概念，并且在美国海军近来的信息保证初步行动中发挥了作用。

前　言

蜂窝移动通信系统已经经历了从模拟技术到数字技术好几代的发展。第一代（1G）移动通信系统是指模拟系统，第二代（2G）移动通信指数字系统，第三代（3G）移动通信指的是增强的数字系统。每一代都已使或将使全社会进入一个更为先进的无线通信阶段。

第一代系统是当用户需要进行移动或无法访问有线网络时的一个替代方案。2G 数字系统和有线服务在某些市场上有时会产生竞争，而在更为成熟的市场上则与有线网络互为补充。今天 3G 的市场目标是，要使有线网络成熟的市场进入随处可见移动终端的饱和状态。

William Webb 在他的一篇题为《未来的无线通信》的文章中，提出未来全球范围内无线通信的持续增长，将会由合并大量不同类型的网络形成一个巨大的虚拟个人局域网来实现。这些系统提供的服务内容将和 3G 系统非常不同。不同类型设备之间的互通能促使更多的无线电设备投入使用，还有利于促进推出许多适于个人使用的新产品。

因特网是一个发展中的公共骨干网络，和大多数新型无线应用密不可分。它不是像 2G 或 3G 技术的基础设施那样的专有无线基础设施。因特网将会通过添加新的特色和增强其移动访问可用性的协议，得以继续发展。对于所有应用，通过 IP 和高数据速率的分组交换来完全取代实时的电路交换连接，在技术上应该是可行的。无线频谱的需求将会增加，并且将用来满足用户对新型无线服务的需求的增长而引起的对带宽要求的增加。Webb 认为，移动通信和因特网的集中和完全的结合将给无线通信在未来的发展提供了可能。移动因特网的使用将会远远超过固定的因特网访问。后者是我们目前所了解的，通过 PC（个人电脑）和调制解调器，或是通过连接到公司服务器和路由器上的 PC 来访问因特网。

两个威胁到无线系统增长的因素是标准化和安全问题。标准化在传统上是通过保证设备之间的兼容性来扩展市场和降低成本，但也有时会起到限制作用。为保证利用 Internet 骨干网的无线系统的安全，提出了无线应用协议（WAP），它就是一个限制型标准的例子。它采取传统蜂窝系统的单一多用途终端的模型。而无线多媒体意味着，存在许多种不同类型的特定应用的终端和设备。标准化过程必须要从保证兼容性转变到允许不相容，例如一般的数字网络和一些专门的应用。

安全问题将会成为 3G 以后技术的推动因素并且也是抑制因素。所有这些预期的无线通信的发展都暗示了一个很大的假设，即电信产业、管理者和政府将会接受，并跨国界地自由分享公开的标准、程序和安全特征。在实践中几乎每一个保护 3G 网络的专用加密系统都曾被攻破过，这也是一个事实。即使这一有趣的事实并没有阻止安全的发展，但这种淡忘在如今的电信系统中是公认的经验并且相当普遍。

欺诈一直是一个长期存在的问题，尤其对于移动无线通信来说。从 1G 到 2G 移动电话改进的主要推动力，是因为盗用移动 ID 号以及非法盗打电话相对容易，使欺诈案越来越多。

数字蜂窝系统克服了这些问题，但是又引入了许多其他欺诈机制。例如偷一个电话，在该机报失之前将电话设为呼叫转移，然后通过转移的方法用本地的价格拨打国际电话。随着无线系统性能的增加，所提供的服务范围也扩大了，欺诈的机会也在增加——服务费用也是如此。如果系统设计者封锁了已知的漏洞（或者没有，这是典型情况），欺诈者还是能发明出新的方案来赚钱。欺诈并不会使无线技术和无线服务的发展停下来，它甚至还可能通过提供强烈的刺激引进新技术而加速其发展。

无线安全

回顾一下关于无线通信系统的研究和目前最好的实践，我们发现有超过 500 种参考资料是有关无线和移动通信系统的设计、技术、管理和市场方面的。然而，没有任何一种将重点集中在无线安全上。因此我们这本书的目的主要是介绍无线安全。我们致力于提供一个平衡的方法，兼顾无线安全以及适用于商业、政府和军事组织的无线安全解决方案。

面向的读者

本书所面向的对象是管理者、决策者、设计人员和项目主管。它有利于这些人尽职地保护其所在机构至关重要的无线信息资产和系统。在 IT 从业者中，对于 CIO（首席信息官）、业务经理、网络工程师、网络主管、数据库管理员、程序员、分析家、EDI 计划者以及其他负责应用适当的 INFOSEC 对策来保护无线应用和安全的专业人士，本书将大有裨益。本书适合于无线计算机安全专业的一年级研究生课程，以及工程/MBA 项目。在本书的参考书目、网址和原文中提供了大量的信息资源，值得进一步阅读。

本书结构安排

本书的目标是探索无线科技、技术和方法这一宽广的领域，提供有关的分析和见解，增进对安全的理解并延长应用的寿命。本书内容分为四个部份。

- 第 1 部份：无线威胁　阐述了无线通信的基本概况以及无线技术、电信、蜂窝网络和传送技术的社会影响。然后根据无线信息战模型提出了无线安全。这部分中有两章内容是关于空中到地面的接口，以及在电话和卫星系统中都普遍存在的脆弱性。
- 第 2 部份：密码对策　涵盖了广泛的各种密码技术，从流密码、椭圆曲线密码（ECC）、到 Rijndael——一个成功的高级加密标准（AES），它可能有效应用在无线通信中。在这一部分还讨论了密码技术的限制以及对强健的认证系统的需求，介绍了语音密码这一很有前景的学科和应用中的密码对策。
- 第 3 部份：应用方案　是一个实践性很强的章节，包含了安全原则和流行的无线技术（例如无线局域网、WAP、TLS、蓝牙和语音 IP）的安全缺陷。
- 第 4 部份：硬件解决方案和嵌入式设计　重点集中在端到端（E2E）安全和最优化实时无线通信安全的硬件考虑上。这部分还讨论了高级集成电路的 E2E 实现，即利用专门的现

场可编程门阵列（FPGA）实现快速的原型开发和技术确认。并且讨论了超大规模集成电路（VLSI）、专用集成电路（ASIC）或 IP 核（IP cores），作为在最新的片上系统（SOC）中实现的解决方案。

致　谢

书是许多人劳动的结晶，而不仅仅是沉思中的作家单独完成的，这本书也不例外。本书经过该领域很多专家的浏览，他们慷慨地给予了本书自己的时间和专家意见，对这本书的出版起了很大帮助。下面这些人审阅了本书的全部或部份手稿。

Booz • Allen and Hamilton 公司副总裁 Mike McConnell，Booz • Allen and Hamilton 公司主要负责人、密码专家 Edward J. Giorgio，Booz • Allen and Hamilton 公司高级管理人员 Joseph Nusbaum，Alfred J. Menezes 教授（《Handbook of Applied Cryptography》一书的作者），还有许多在 THLC 的同事和朋友。特别是执行总裁 Bruce Young，Chad Rao——SW 工程副总裁，Ronald H LaPat——系统工程副总裁，Edward D'Entremont——商业发展部副总裁，Krishna Murthy——SW 工程董事，执行副总裁 Thomas J. Petrarca。还有 GWU-SEAS 部主席 Tom A Mazzuchi 教授，GWU-SEAS 教授 Lile Murphree，GWU-SEAS 教授兼律师 Daniel J. Ryan，GWU-SEAS 教授 Julie J.C.H. Ryan，Georgetown 大学信息安全技术教授 Dorothy Denning，退休教授 I. J. Kumar 博士，Shri Kant 教授，UARK 退休教授 Charles M. Thatcher，TAMU 教授 R. W. Serth，Waldo T. Boyd 高级编辑，创意写作所有者兼高级密码专家，Robert V. Klauzinski、Mintz 以及其他知识产权律师，McGraw-Hill 专业图书高级主编 Marjorie Spencer，MacAllister 出版处项目经理 Beth Brown，RSA 安全部门的 Mark Luna。

特别要提到 THLC 的“加州”小组。感激他们的努力、检查、建议和为我们付出的辛勤劳动。我们要特别感谢：Sujatha Durairaj，Ramana Anuganti，Srisailam Narra，Prasanthi Tallapaneni，Sirisha Kota，Shiva Shankar Manjunatha，Venu Anuganti 和 Sridhar Choudary Chadalavada。

无法忘记我们的好朋友 Naidu Mummidi。在写这本书时，Naidu 很意外地英年早逝，年仅 30 岁，我们这些认识而且曾经与他密切合作的人都深感悲痛。愿他能够安息！我们永不会忘记他。

我们也要感谢密码学家 John Burroughs 博士所给予的帮助，他给我们的工作提出了许多建设性意见。Shayle Hirschman 辛勤努力的工作以及他在电路细节方面的敏锐眼光也特别值得我们感谢。Natural Microsystems 的 Kevin Bruemmer 也无私地给予了我们一些建设性意见，他的专家意见给人以深刻的印象。衷心感谢他和我们曾经进行的一些极其有趣的探讨。来自 Brown 大学和 NTRU 的教授 Joe Silverman 和 Worcester Polytechnic 学院的教授 Christof Paar，同样还有来自 Oregon 州立大学的 CetinKoç 教授和 Erkay Savas 博士，伊斯坦布尔 Sabanci 大学的 Yusuf Leblebici 教授，都针对嵌入式安全系统提出了对一些特定方法的见解，分享了彼此的想法。还要感谢 Thomas ollinger 和 Kumar Murthy 教授。作者还要感谢加州大学洛杉矶分校（UCLA，University of California Los Angeles）电子工程系的 Ingrid Verbauwhede 和位于

弗吉尼亚 Fairfax 的 George Mason 大学电子和计算机工程系 Kris Gaj 教授同意我们多次引用他们关于用高效硬件实现密码算法的最优方法这一令人瞩目的研究成果。感谢加拿大安大略的滑铁卢大学应用密码研究中心教授 Guang Gong 博士，他给我们进行了很多咨询，花费了大量时间解决我们的问题。还要感谢位于芬兰 Oulu 市的 Oulu 大学无线通信中心的 Kări Kärkkäinen 博士以及美国 Massachusetts 州 Worcester 市 WPI 大学 ECE 系的 Thomas Wollinger。最后，我们还要感谢位于匈牙利首都布达佩斯的 AZ Kando 学院的退休教授 Mihály Toth 博士给我们的鼓励和意见。

Nichols 教授在美国华盛顿特区 George Washington 大学（GWU）2000-2001 年秋季、春季和夏季教授信息安全和密码系统研究生课程：应用、管理和策略。他的许多信息安全方向的资格认证学生、硕士生和博士生都自愿组队，开展强化研究，帮助我们完成了本书好几章内容的写作。为了使本书成为 GWU 的一门信息安全硕士和资格认证项目的新选修课的首选教材，许多人积极和我们进行合作。特别要提到的这些有才能和奉献精神的专业人士在贡献者列表部分做了介绍。

最后要感谢 Montine Nichols 对终稿的贡献以及对本书进行了审稿。Joe Schepisi 的词汇表做得很好，Dennis Kezer 是我们收集和统计参考文献的倡导者。感谢 Andrew Downey 提供了这本书内整理过的 RSA 2001、RSA ASIA 2001 和 GWU INFOSEC 2001 材料。还有一些我们可能会忘记但应该感谢的人，我们感激他们提供的相关观点、建议和忠告。我们自己难免也会出现各种错误，如果读者发现，请发 E-mail 到 comsec@epix.net 或 crypto@gwu.edu 告诉作者出现的错误，我们将竭力改正这些错误，发布勘误表。

Randall K. Nichols
George Washington University
School of Engineering and Applied Sciences (SEAS)
Washington，DC
&
Chief Technical Officer
INFOSEC Technologies，LLC
Cryptographic / Anti-Virus / Anti-Hacking
Computer Security Countermeasures
Carlisle，PA
November，2001
Website: www.infosec-technologies.com
Email: cto@infosec-technologies.com
Voice: 717-258-8316
Fax: 717-258-5693
Cell: 717-329-9836

Panos C. Lekkas
Chief Technology Officer & General Manager
Wireless Encryption Technology Division
TeleHubLink Corporation (THLC)
wireless_security@attglobal.net
Marlboro，MA
November，2001

作 者 简 介

Randall K. Nichols

常务编辑/作者

Randall K. Nichols（A.K.A. LANAKI）是 INFOSEC 科技公司的首席技术官（CTO）。这是一家咨询公司，专门从事密码、反病毒、反黑客的计算机安全措施，为其商业客户和政府客户提供信息安全（INFOSEC）的需求支持。

先前，Nichols 担任 TeleHubLink 公司（THLC）密码方面的副总裁。他领导 THLC 的密码研究和高级密码技术的开发活动。他是 THLC 取得专利的基于 HORNET™SHA 的加密技术的合作者，该技术被嵌入到一系列高级专用集成电路（ASIC）、现场可编程门阵列（FPGA）以及 THLC 公司卖给无线和电话行业客户的 IP 核（IP cores）中。

在进入 TeleHubLink 公司之前，Nichols 是 COMSEC Solutions 公司的首席执行官（CEO）。这是一家从事密码/反病毒/生物测定对策的公司，最终被 TeleHubLink 公司并购。COMSEC Solutions 公司给大致 1200 个商业、教育以及美国政府客户提供客户支持。

Nichols 为 McGraw-Hill 的加密和信息安全专业图书担任丛书编辑。以前 Nichols 任国际计算机安全协会（ICSA）密码和生物测定学的技术总监。Nichols 还担任过美国密码协会（ACA）的总裁和副总裁。Nichols 享誉国际，在密码和 INFOSEC 计算机应用（在工程、咨询、建筑和化工行业）方面有 38 年的领导经验。

Nichols 教授在位于华盛顿特区的著名的乔治华盛顿大学的工程管理和应用科学（SEAS）学院教授信息安全、密码、系统应用管理及策略这几门研究生课程。他还在位于弗吉尼亚 Quantico 的 FBI 国家研究院教过密码学。Nichols 是一个专业演讲者，常常给专业研讨会、国际技术会议、学校以及内部的客户提供密码和信息安全方面的信息。

本书是 Nichols 教授在密码和信息安全方面的第 5 部著作。《保护你的数字资产不受黑客解密高手、间谍和盗贼的袭击》（McGraw-Hill 专业图书，1999，ISBN：0-07-212285-4）一书是他在密码和信息安全对策方面最畅销的书。该书被用作乔治华盛顿大学、詹姆士迈迪逊大学、新泽西 Rowan 学院、爱荷华州立大学、东部密歇根州立大学和韩国 Yonsei 大学的研究生信息安全课程的课本。《ICSA 密码指南》（McGraw-Hill 专业图书，1998，ISBN：0-07-913759-8）和《古典密码课程，卷 I 和卷 II》（分别是 Aegean Park 出版社，1995，ISBN：0-89412-263-0 和 1996，ISBN：-89412-264-9）两书令 Nichols 获得的业界的认可，为他赢得了在业界的声誉。期待着 Nichols 的下一部作品《信息站和恐怖行动》尽快问鼎书市。

Panos C.Lekkas

Lekkas 先生是 TeleHubLink 公司的首席技术官，无线加密技术部门总经理。在他进入 THLC 之前，Lekkas 先生在几个尖端高科技公司担任技术和企业管理职位。

他是 Encryption.com 公司的共同创始人、总裁和 CEO。这是一家设计通信安全集成电路的公司，该公司在被 THLC 并购前就已经开发了 HORNET™安全技术。在此之前，他是 ACI 的策划副总裁，从事设计和仿真高级通信安全和数字信号处理微芯片，TCC 商业开发部总监，指导新产品的界定以及设计硬件加密和密钥管理系统，用于政府和商业的高速通信领域。

作为 Galileo 公司国际销售和市场部总监，Lekkas 先生开发了高级电子光学和光纤光学技术方面的新应用和新市场：适用于军事夜视能力的图像增强系统，军用电子设备的智能显示以及用于质谱分析和核科学的科学探测系统。他对于 WDM、搀杂少量杂质的氟化物光纤电信放大器技术以及在线式光纤光学傅里叶变换红外光谱仪（FTIR）在日本和欧洲市场上的投放，都发挥了作用。

Lekkas 先生最初加入 Galileo 公司是为了建立其欧洲分公司，他成功地经营了该公司好几年。在这之前，Lekkas 在 IBM 工作过几年，其间曾在美国和欧洲分部担任过多个职务。作为德州 Austin 的首席系统工程师，他协助引入了最终成为了著名 RS/6000 超级计算机核心的 RISC 体系。在他的早期工作生涯中，他是 Silvar-Lisco 公司的一个 VLSI 设计和 EDA 应用工程师。

Lekkas 先生在德州休斯顿的 Rice 大学所做的硕士研究是激光量子电子学和半导体工程。他获得了两个电子工程硕士学位，一个是无线通信与天线，另一个是 VLSI 设计。Lekkas 还在公司赞助下在比利时 Catholic University of Leuven 攻读了 MBA 课程。他在希腊雅典的雅典国立科技大学获得了电子工程学士学位。他是欧盟批准的教授工程师，也是 IEEE 和美国数学社团会员。

Lekkas 先生在欧州、日本、亚洲和中东都工作过。他能流利地讲 18 个国家的语言，包括法语、德语、荷兰语、瑞典语、芬兰语、俄语、希伯来语、波斯人语、日语、乌尔都语、印度尼西亚语、马来语、西班牙语、北印度语、孟加拉语、韩语、汉语普通话，当然还有希腊语。在他宝贵的闲暇时间，他对古典音乐很着迷，还喜欢研究各国历史、高级语言学、认知神经系统学和飞机学。

目　录