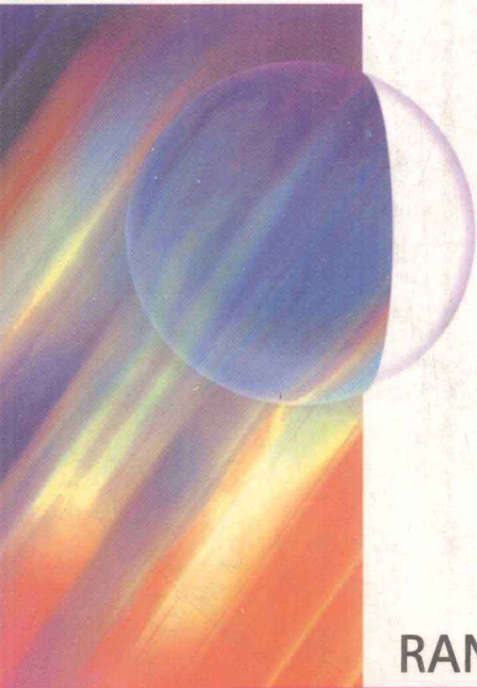


McGraw-Hill TELECOM
P R O F E S S I O N A L

WIRELESS SECURITY

Models, Threats, and Solutions



Learn to recognize the threats and vulnerabilities unique to wireless communications

Plan application-aware cryptographic defenses and review available solutions

Specify defenses for telecom, broadband, satellite, and other markets soon to come

RANDALL K. NICHOLS • PANOS C. LEKKAS

INTERNATIONAL EDITION

Wireless Security

Models, Threats, and Solutions

**Randall K. Nichols
Panos C. Lekkass**

McGraw-Hill

Boston Burr Ridge, IL Dubuque, IA Madison, WI New York San Francisco St. Louis
Bangkok Bogotá Caracas Kuala Lumpur Lisbon London Madrid Mexico City
Milan Montreal New Delhi Santiago Seoul Singapore Sydney Taipei Toronto

McGraw-Hill



A Division of The McGraw-Hill Companies

WIRELESS SECURITY

Models, Threats, and Solutions

International Edition 2002

Exclusive rights by McGraw-Hill Education (Asia), for manufacture and export. This book cannot be re-exported from the country to which it is sold by McGraw-Hill. The International Edition is not available in North America.

Copyright © 2002 by The McGraw-Hill Companies, Inc. All rights reserved. Except as permitted under the United States Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a data base or retrieval system, without the prior written permission of the publisher.

Some ancillaries, including electronic and print components, may not be available to customers outside the United States.

Throughout this book, trademarked names are used. Rather than put a trademark symbol after every occurrence of a trademarked name, we use names in an editorial fashion only, and to the benefit of the trademark owner, with no intention of infringement of the trademark. Where such designations appear in this book, they have been printed with initial caps.

Notice: Information contained in this work has been obtained by The McGraw-Hill Companies, Inc. ("McGraw-Hill") from sources believed to be reliable. However, neither McGraw-Hill nor its authors guarantees the accuracy or completeness of any information published herein, and neither McGraw-Hill nor its authors shall be responsible for any errors, omissions, or damages arising out of use of this information. This work is published with the understanding that McGraw-Hill and its authors are supplying information but are not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought.

10 09 08 07 06 05 04 03 02 01

20 09 08 07 06 05 04 03 02

CTF BJE

Cataloging-in-Publication Data is on file with the Library of Congress.

ISBN 0-07-138038-8

When ordering this title, use ISBN 0-07-120707-4

Printed in Singapore

Foreword

The safeguarding of information traveling over wireless technology has quickly become one of the most important and contentious challenges facing today's technology innovators. With the advent of *third generation* (3G) Internet technology—a capability that connects mobile devices to the Internet and allows users to send and receive detailed information over wireless and fiber networks—the security measures necessary to protect critical data on these wireless networks have become even more elusive and complex. The issues surrounding proper security in the use of networked wireless devices have played out in a contest between individual, business, and government interests. While protecting the privacy of individuals is of utmost importance, many would argue individual privacy must be balanced with the interests of public safety and law enforcement's ability to monitor the private communications of suspected criminals. Moreover, the business costs associated with providing the appropriate security measures are often substantial.

Current security issues are further clouded by the merging of the private and public information infrastructure sectors, areas previously guided by separate regulatory measures that now exchange information and operate in a common framework known as the *public switched network* (PSN). Wireless technology has evolved to carry increasing amounts of valuable information that require higher privacy and security levels. Some refer to the PSN as the “Interstate Highway” system for telecommunications; however, wireless increasingly serves as the “on-and-off ramps” to this vast and global information infrastructure.

From my vantage point of a career in Naval and National Intelligence focused on developing intelligence on the former Soviet Union and hot spots impacting U.S. national security interests, the interception of wireless communications was key to our successful intelligence operations. This was true during World War II, throughout the Cold War, and it continues today. Data in the form of wireless communications in the days before digital, computer-based networks was vulnerable only during the moment of transmission. It was in that instant of transmission that the intelligence needed to be collected, or the opportunity was lost. Intelligence officers learned to rely on communications intelligence from wireless systems as a means of providing invaluable strategic and tactical intelligence. Experience taught us that wireless communications had to be protected at the precise moment that tactical, and even critical, strategic information was being communicated. The successes of Desert

Storm in the Gulf War further demonstrated how wireless communications could be turned into immediate actionable intelligence unavailable from any other source. Today, massive networking, with data created, transmitted, and stored online, has made connected nations the world's most vulnerable target for information attack. These vulnerabilities include capture of information for intelligence purposes, disruption or corruption of information, or destruction of data in the network. Because this networking capability, which has added to productivity, efficiency, and wealth creation, carries so much vital data, such nations have significantly more to lose than their less developed counterparts. For example, terrorists potentially could target the monetary system, a networked infrastructure that moves and records financial transactions. The vast majority of this wealth is stored in a database, which is vulnerable to disruption from a sophisticated and determined adversary.

As we expand and enhance our connectivity, our vulnerability to hostile attack inside the homeland will only increase. Military superiority will not entirely provide the protection we have become accustomed to in the past. Rogue states, terrorists, and other disaffected groups have the ability to acquire cyber weapons of mass disruption, and the means of their implementation have multiplied. As the recent Hart-Rudman Report on National Security for the 21st Century ominously predicted, without adequate safeguards, a catastrophic event inside the U.S. will occur. With new digital network information technology, our borders will become more porous; some will bend and some will break. U.S. intelligence will face more challenging adversaries, and even the best intelligence measures will not prevent all surprises. Reliance on unprotected networks carries with it the risks of loss of government services and military failure, as well as catastrophic economic consequences.

The military is increasingly dependent on the private information infrastructure to conduct its essential operations. This dependence is complicated by custom, culture, and statutes that focus the military on foreign operations and would restrict any attempt to prevent or contain asymmetric attacks within borders. In the future, collaboration and coordination between civil, military, and private sectors will become essential. In time, data will have to be shared for rapid integration into information products to be useful to operational decision makers. Likewise, government supplied information will have to flow to the private sector to ensure appropriate awareness and decision-making.

Increased mobility has become a key benefit to an Internet-working society. With the past and current proliferation of mobile technologies and devices, vendors have moved aggressively to extend the wired network through mobile pathways that businesses and service providers can operate with confidence. The value for mobile wireless users resides with the ability to communicate over great distances, while in motion, at a relatively modest cost. With so much of our national wealth riding in the networks using wireless devices for entry and exit, it is clear that more attention needs to be paid to building in the required security features. Furthermore, a new security culture needs to emerge across the entire Internet user community. We must resist the glorification of the hacker ethic, in which destructiveness poses as inquisitiveness. In a personal vein, we need to develop a culture that emphasizes responsibility and accountability on the part of every user—from school child to CEO.

Proper online security habits must become second nature to protect our privacy and the broader interests of society. These include all of the obvious things that we should do, but often don't: changing passwords; disconnecting from the Internet when it is not in use; running anti-virus software daily; changing the default password whenever a new device is purchased; and using appropriate security and encryption services. In addition to personal action, corporations must understand and adopt proper security technology to safeguard the future. Nowhere is the development of this new security culture more important than in the wireless theater of operations.

Wireless Security addresses these evolving security concerns by providing deep insights in a readable and effective manner. The broad practical and academic backgrounds of the authors have allowed them to seamlessly present the most current state of information protection and vulnerabilities related wireless security in a balanced, easy to understand and fully documented treatise. The cases presented are real and topical, and flow seamlessly with the theme of the subject matter presented. The authors tell the reader the risks, examine cases where people and systems have fallen victim, and provide remedies to those who have been victimized by these risks.

Readers will find that the authors have taken an approach of best business practices to present their material—a balanced identification of technologies combined with a systems approach to the problem of wireless communications security. The book is designed for readers who operate at the executive, policy, or managerial level and who have responsibility for protecting their organization's information assets, intellectual property, and communications systems. The content presented is equally valuable to both private sector and government managers.

Wireless Security provides a reasoned approach to making sound decisions about how to expend scarce resources in order to achieve a balanced multidisciplinary approach to wireless security. The end result is a necessary and attainable security response for organizations and government alike.

J. M. (Mike) McConnell, Vice Admiral, USN (Retired)

Vice President, Booz • Allen & Hamilton, Inc.

Former Director of the National Security Agency (NSA), 1992–1996

About J. M. (Mike) McConnell

As a Vice President at Booz-Allen & Hamilton, Inc., Mr. McConnell leads assignments in Information Assurance for departments and agencies of the federal government and for commercial clients. In addition, he oversees the firm's Information Operations assignments for the Department of Defense. From 1992 to 1996, Mr. McConnell was Director of the *National Security Agency* (NSA), the U.S. agency responsible for Signals Intelligence and all security services that protect classified Government information. He also served as the Intelligence Officer for the Chairman, Joint Chiefs of Staff during the dissolution of the Soviet Union and Operation Desert Storm.

At Booz • Allen & Hamilton, Mr. McConnell has led assignments for the Presidential Commission on Critical Infrastructure Protection focused on security standards in the Banking and Financial Industry. He also led work with the U.S. *Critical Infrastructure Assurance Office* (CIAO) for the White House; his team developed the National Infrastructure Assurance Plan design and planning guidelines. Mr. McConnell helped the Department of Justice/FBI develop the new *National Infrastructure Protection Center* (NIPC) concept of operations and was instrumental in the Navy's recent information assurance initiatives.

Preface

Cellular systems have evolved through several generations characterized by analog or digital technologies. *First generation* (1G) refers to analog systems, *second generation* (2G) to digital, and *third generation* (3G) to enhanced digital. Each generation moved the industry into a more advanced stage of wireless communications.

The 1G systems were an alternative when a user needed to be mobile or wired systems were not available. The 2G digital systems were partially competitive with wired services in some markets and were complementary to wired in more mature markets. The goal of today's 3G markets is to drive the wired mature markets into saturated ones in which mobile terminals are ubiquitous.

William Webb in his excellent text, *The Future of Wireless Communications*, suggests that future sustained growth in the wireless global theater will be accomplished by aggregating large numbers of different kinds of networks into an enormous number of virtual personal area networks. *Content* in these systems will be very different from that of 3G systems. Enabling devices to talk to each other is what allows more wireless devices to be sold and the impetus for many new products in adaptive personal areas.¹

One common evolving backbone network, which is the glue to most new wireless applications, is the Internet. It is not a proprietary wireless infrastructure as is the basis of 2G or 3G technologies. The Internet will continue to evolve through new features and protocols that enhance its usability for mobility access. A complete replacement of real-time circuit-switched connections for all applications through IP and packet-switching at high data rates should be technically feasible. Radio spectrum requirements will increase and be provided to meet increased bandwidth demands posed by increased users, usage, and new wireless services. Webb predicts that a convergence and thorough integration of mobile communications and the Internet makes future wireless growth possible.² Mobile Internet usage will far surpass stationary Internet access, as we know it today, through desktop PCs and modems or PCs connected to corporate servers and routers.³

Two factors that threaten the growth of wireless systems are standards and security. Standards traditionally expand markets and lower costs by assuring equipment to be interoperable, but they can be confining too. The *wireless applications protocol* (WAP) proposed for secure wireless systems using the Internet backbone is an example of a confining standard. It assumes the one terminal-for-everything

model of traditional cellular practice. Wireless multimedia implies many different kinds of application-specific terminals and appliances. The standardization process must change from one that assures compatibility to a process that enables incompatibility such as generic digital networks and proprietary applications.⁴

Security will be both the enabler and inhibitor of the post-3G world. All this expected wireless growth implies a huge assumption that the telecommunications industry, regulators, and governments will accept open standards, processes, and security features and freely share them across international borders. It is also a fact that practically every proprietary encryption system protecting 3G networks has been cracked. Even this interesting fact has not stopped the proliferation of security by obscurity that is accepted practice and prevalent in today's telecommunications systems.

Fraud has been an enduring problem, especially for mobile radio. Much of the impetus for the move from 1G to 2G mobile phones was the increasing fraud occurring because of relative simplicity of stealing mobile identification numbers and making illegal telephone calls. Digital cellular systems overcame these problems but enabled a number of other fraudulent mechanisms, such as stealing a phone and setting up call forwarding before the phone theft is reported and then making international calls on the forwarded path at local rates. As the capabilities of wireless systems increase along with the range of services offered, the opportunities for fraud increase—and so do the attendant costs. As systems designers close off the known loopholes (or don't, which is the typical case), fraudsters seem to devise new schemes to make money. Fraud will not stop the development of wireless technology and services. It may even speed up the overall development by providing strong incentives to introduce new secure technologies.⁵

Wireless Security

A review of the research about wireless communications systems and current best practices turned up more than 500 references in the design, technology, management, and marketing of wireless and mobile communications systems. However, there was not one reference devoted to wireless security. That then became the goal of our book. We have endeavored to provide a balanced approach to wireless security and wireless security solutions for commercial, government, and military organizations.

Target Audience

Wireless Security is for the manager and policy maker, the designer and the project lead. It was written for the benefit of those who must exercise due diligence in protecting the valuable wireless information assets and systems upon which their organizations depend. Among IT practitioners, it is valuable to CIOs, operations managers, network engineers, network managers, database managers, programmers, analysts, EDI planners, and other professionals charged with applying appropriate INFOSEC countermeasures to secure wireless applications and devices. *Wireless Security* is suitable for a first-year graduate course in wireless computer

security, for computers-in-business courses, and for Engineering/MBA programs. There are plenty of resources in the bibliography, URL references, and textual leads to further reading.

Structure of This Book

The goal of *Wireless Security* is to explore the vast array of wireless technologies, techniques, and methodologies; to provide relevant analysis and understanding; and to improve the thoughtfulness and longevity of implementations. *Wireless Security* is divided into four parts:

- *Part I: Wireless Threats* presents a basic overview of wireless communications and societal impacts of wireless, telecommunications, cellular network, and bearer technologies. Wireless security is then presented in terms of the model of Wireless Information Warfare. Two chapters inspect the air-to-ground interface and vulnerabilities that are prevalent in both telephone and satellite systems.
- *Part II: Cryptographic Countermeasures* covers a wide range of encryption technologies from stream ciphers to *elliptic curve cryptography* (ECC) to Rijndael, the *advanced encryption standard* (AES) winner that may be applied effectively to wireless communications. The limitations of encryption and need for robust authentication systems are discussed. The fascinating science of speech cryptology is introduced to balance the cryptographic countermeasures applied.
- *Part III: Application Solutions* is a practical section covering the security principles and flaws of popular wireless technologies such as wireless LANS, WAP, TLS, Bluetooth, and VOIP.
- *Part IV: Hardware Solutions and Embedded Design* focuses on hardware considerations for *end-to-end* (E2E) security and optimizing real-time wireless communications security. E2E implementations with advanced integrated circuits; namely, using specialized *field programmable gate arrays* (FPGAs) for rapid prototype development and technology validation and *very-large scale integration* (VLSI) *application-specific integrated circuits* (ASICs) or *intellectual property* (IP) cores for the solution implementation in state-of-the-art *systems-on-a-chip* (SOC) are discussed.

Endnotes

¹William Webb, *Wireless Communications*, Artech House, 2001, pp. 245–246.

²*Ibid.*, p. 277.

³*Ibid.*, p. 277.

⁴*Ibid.*, p. 266.

⁵*Ibid.*, pp. 133–134.

Acknowledgments

Books such as this are the products of contributions by many people, not just the musings of the authors. *Wireless Security* has benefited from review by numerous experts in the field, who gave generously of their time and expertise. The following people reviewed all or part of the manuscript: Mike McConnell, Vice President for Booz • Allen and Hamilton and previous Director National Security Agency; Edward J. Giorgio, Principal for Booz • Allen and Hamilton and previous Chief Cryptographer and Cryptanalyst for the National Security Agency; Joseph Nusbaum, Senior Manager for Booz • Allen and Hamilton; Professor Alfred J. Menezes, author of *Handbook of Applied Cryptography*; and plenty of colleagues and friends at THLC. More specifically, Bruce Young, CEO; Chad Rao, Vice President—SW Engineering, Ronald H. LaPat, Vice President—Systems Engineering; Edward D'Entremont, Vice President—Business Development; Krishna Murthy, Director—SW Engineering; Thomas J. Petrarca, Executive Vice President. Also GWU-SEAS Department Chair, Professor Tom A. Mazzuchi; Professor Lile Murphree at GWU-SEAS; Professor and attorney Daniel J. Ryan, at GWU-SEAS; Professor Julie J.C.H. Ryan at GWU-SEAS; Dorothy Denning, Professor of INFOSEC Technology at Georgetown University; Emeritus Professor Dr. I. J. Kumar; Professor Shri Kant; Professor Emeritus, Charles M. Thatcher, UARK; Professor R. W. Serth, TAMU; Waldo T. Boyd, senior editor, Creative Writing, Pty. and senior cryptographer; Robert V. Klauzinski, intellectual property attorney for Mintz, et al; Marjorie Spencer, senior editor for McGraw-Hill Professional Books; Beth Brown, project manager for MacAllister Publishing Services; Mark Luna at RSA Security.

Special mention is made of THLC's "California" team. We appreciate their efforts, reviews, comments, and hard work on our behalf. Specifically we thank: Sujatha Durairaj, Ramana Anuganti, Srisailam Narra, Prasanthi Tallapaneni, Sirisha Kota, Shiva Shankar Manjunatha, Venu Anuganti, and Sridhar Choudary Chadavalada.

Our dear friend Naidu Mummidi is especially remembered. While we were writing this book, Naidu left this life so prematurely and so unexpectedly at the age of 30, filling the hearts of all of us who knew him and worked closely with him with tremendous sorrow. May he rest in peace! We pray for his soul and for his family. We will never forget him.

We also respectfully acknowledge the help of Dr. John Burroughs, previously Chief Cryptographer of the National Security Agency, for his many constructive comments on our work. Shayle Hirschman deserves a special note of thanks for his hard and diligent work as well as for his hawkish eye for circuit detail. Kevin Bruemmer of Natural MicroSystems has been gracious in sharing thoughts and his impressive expertise. Some extremely interesting discussions with him are sincerely appreciated. Professor Joe Silverman from Brown University and NTRU, as well as Professor Christof Paar, Worcester Polytechnic Institute, Professor Cetin Koç and Dr. Erkey Savas, both of Oregon State University, as well as Professor Yusuf Leblebici, Sabanci University, Istanbul, all provided insight and shared thoughts on specific approaches to embedded security systems. Our thanks go to Thomas Wollinger and Professor Kumar Murthy. The authors are grateful to Professor Ingrid Verbauwhede of the Electrical Engineering Department at the *University of California, Los Angeles* (UCLA) and to Professor Kris Gaj of the Electrical and Computer Engineering Department at George Mason University, in Fairfax, Virginia, for their permission to refer extensively to their impressive research work regarding optimal implementations of cryptographic algorithms in efficient hardware. We thank Professor Dr. Guang Gong of the Center of Applied Cryptographic Research, University of Waterloo, Ontario, Canada, for extensive consultations and numerous hours of problem solving and coding. Our thanks also go to Dr. Kari Kärkkäinen of the Center of Wireless Communications, University of Oulu, Oulu, Finland, and to Thomas Wollinger of the ECE Department at WPI, Worcester, Massachusetts. Last, we thank Professor Emeritus, Dr. Mihály Toth, AZ Kando College, Budapest, Hungary, for his encouragement and reviews.

Many of Professor Nichols' INFOSEC certificate, masters, and doctorate students from his 2000–2001 Fall, Spring, and Summer graduate courses in *INFOSEC* and *Cryptographic Systems: Application, Management and Policy* at The George Washington University (GWU) in Washington, D.C., voluntarily formed teams, performed intensive research, and assisted with the writing of several chapters of *Wireless Security*. We worked passionately and cooperatively toward the goal of making *Wireless Security* the premier textbook for a new elective course in the information security Masters and certificate programs at GWU. Special mention of these talented and dedicated professionals is made in the List of Contributors section.

Finally, Montine Nichols deserves a commendation for her help on the final drafts and copy edit for our book. Joe Schepisi did a fine job on the Glossary, and Dennis Kezer was the prime mover for the collection and aggregation of our References. We thank Andrew Downey for his assistance on our material presentation for RSA 2001, RSA ASIA 2001, and GWU INFOSEC 2001 tune-up. To these and

many others to whom we may have failed to give appropriate credit, we are grateful for their relevant ideas, advice, and counsel. Any mistakes or errors are, of course, our own. Please advise the authors of errors by e-mail to comsec@epix.net or crypto@gwu.edu and we will do our best to correct the errors and publish an errata list.

Randall K. Nichols
Professor, The 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

List of Contributors

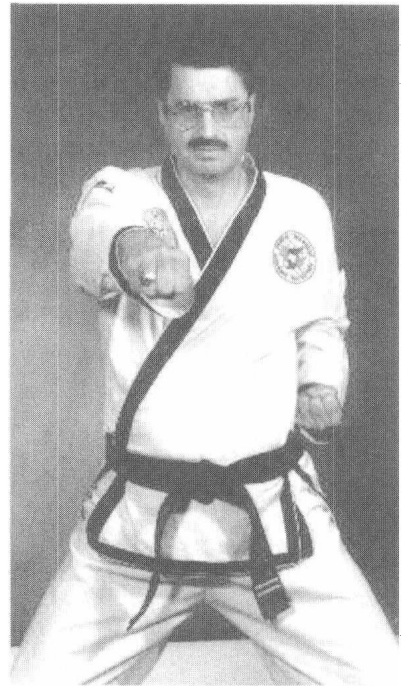
The authors express their gratitude to the talented review teams and The George Washington University research teams from the *School of Engineering Management and Applied Science* (SEAS), Washington, D.C., who contributed so much of their time and expertise to make *Wireless Security* a success. With deepest respect, we present the qualifications of our teammates.

Authors

Randall K. Nichols **Managing Author/Editor**

Randall K. Nichols (a.k.a. LANAKI) is Chief Technical Officer of INFOSEC Technologies, a consulting firm specializing in Cryptographic, Anti-Virus, and Anti-Hacking computer security countermeasures to support the information security (INFOSEC) requirements of its commercial and government customers.

Previously, Nichols served as Vice President—Cryptography, for TeleHubLink Corporation (THLC). Nichols led TeleHubLink Corporation's cryptographic research and development activities for the company's advanced cryptographic technology. He was co-author of THLC's patented HORNET™ SHA-based encryption technology, which is embedded into a family of advanced application-specific integrated circuits (ASIC's), field programmable gate arrays (FPGA) and IP cores that THLC sells to wireless and telephone industry customers.



Prior to joining TeleHubLink Corporation, Nichols was CEO of COMSEC Solutions, a cryptographic/anti-virus/biometrics countermeasures company that was acquired by TeleHubLink Corporation. COMSEC Solutions provided customer support on INFOSEC to approximately 1,200 commercial, education, and U.S. government clients.

Nichols serves as Series Editor for Encryption and INFOSEC for McGraw-Hill Professional Books. Nichols previously served as Technology Director of Cryptography and Biometrics for the International Computer Security Association (ICSA). Nichols has served as President and Vice President of the American Cryptogram Association (ACA). Nichols is internationally respected, with 38 years of experience in a variety of leadership roles in cryptography and INFOSEC computer applications (in the engineering, consulting, construction, and chemical industries).

Professor Nichols teaches graduate-level courses in INFOSEC, Cryptography, and in Systems Applications Management and Policy at the School of Engineering and Applied Science (SEAS), at the prestigious George Washington University in Washington, D.C. He has taught cryptography at the FBI National Academy in Quantico, VA. Nichols is a professional speaker and regularly presents material on cryptography and INFOSEC at professional conferences, international technology meetings, schools, and client in-house locations.

Wireless Security is Professor Nichols' fifth title on cryptography and INFOSEC. *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves* was his best-selling book on the subjects of cryptography and INFOSEC countermeasures (McGraw-Hill Professional Publishing, 1999, ISBN: 0-07-212285-4). *Defending* is used as the graduate INFOSEC textbook at the George Washington University, James Madison University, Rowan College of New Jersey, Iowa State University, Eastern Michigan State University, and Yonsei University, Korea. Nichols' previous books, *The ICSA Guide to Cryptography* (McGraw-Hill Professional Books, 1998, ISBN: 0-07-913759-8) and *Classical Cryptography*

Course, Volumes I and II (Aegean Park Press, 1995, ISBN: 0-89412-263-0 and 1996, ISBN: 0-89412-264-9, respectively), have gained recognition and industry respect for Nichols. Expect Nichols' next title, *IN-FOWAR and Terror* to hit the bookstores in early 2002.



Panos C. Lekkas

Mr. Lekkas is the Chief Technology Officer of TeleHubLink Corporation, and General Manager of its Wireless Encryption Technology Division. Prior to his association with THLC, Mr. Lekkas held several technical and business management positions with cutting-edge high-tech companies.

He was cofounder, President, and CEO of wireless Encryption.com, a startup company designing communications security integrated circuits, which began development of the HORNET™ security technology before being acquired by THLC. Prior to that, he was VP of Engineering for ACI, designing and simulating advanced communications security and digital signal processing microchips, and Director of Business Development with TCC, supervising new product definition and engineering for hardware encryption and key management systems used in high-speed government and commercial communications worldwide.

As Director of International Sales & Marketing with Galileo Corporation, Mr. Lekkas developed new applications and markets for advanced electro-optics and fiber optics technologies used in image-intensification systems for military night vision, heads-up displays for military avionics, and scientific detection systems used in mass spectroscopy and nuclear science. He was instrumental in the launch of their WDM, rare-earth-doped-fluoride fiber telecom amplifier technology and online fiber optic FTIR spectroscopy in Japan and Europe.

Mr. Lekkas originally joined Galileo to establish their European branch, which he ran successfully for several years. Before that, Mr. Lekkas spent several years at IBM, a company in which he has held many positions both in the United States and Europe. As Lead Systems Engineer in Austin, Texas, he helped introduce the RISC architecture that ultimately became the heart of the famous RS/6000 supercomputers. Earlier in his career, he was a VLSI design and EDA applications engineer with Silvar-Lisco.

Mr. Lekkas did graduate research in laser quantum electronics and semiconductor engineering at Rice University in Houston, Texas. He has two graduate degrees in electrical engineering, one in wireless communications and antennas and one in VLSI design. Mr. Lekkas has also pursued M.B.A. work in Corporate Finance at the Catholic University of Leuven in Belgium. His undergraduate degree in electrical engineering was earned at the National Technical University of Athens in Athens, Greece. He is a Licensed Professional Engineer in the European Union and a member of the *Institute of Electrical and Electronics Engineers* (IEEE) and of the *American Mathematical Society* (AMS).

Mr. Lekkas has worked in Europe, Japan, Asia, and the Middle East. He is fluent in 18 languages, including French, German, Dutch, Swedish, Finnish, Russian, Hebrew, Persian, Japanese, Urdu, Indonesian, Malay, Spanish, Hindi, Bengali, Korean, Mandarin, Chinese, and, of course, Greek. Married with four children, he lives in the Greater Boston area. In his precious free time, he is an obsessive classical music lover and enjoys studying world history, advanced linguistics, cognitive neuroscience, and airplanes.

The George Washington University Research Teams

The authors are indebted to the superb graduate students of Professor Nichols' EMSE 218 and EMSE 298, INFOSEC, Cryptography and Systems Applications Management and Policy courses from Fall 2000 to Summer 2001 at The George

Washington University, Washington DC, for their voluntary contributions to *Wireless Security*. It became a joint mission for these dedicated and talented people to help create a book that would serve as the first textbook for a new elective course in wireless security proposed for use in the *School of Engineering Management and Applied Science* (SEAS) INFOSEC Masters and Graduate INFOSEC Management Certificate programs. Graduate students were divided into teams and worked in co-operative rather than competitive mode. The research results were outstanding. The management of this talented team was a significant effort. Presented in alphabetical order are personal vitas of these talented people:

GARY L. AKIN is a program/project management official for acquisition, communications, satellite, and automated data processing systems with over 36 years in government service. Twelve of these years were spent abroad in Europe, Africa, and the Middle East. Currently, he is employed with the Defense Information Systems Agency, Information Assurance Program Management Office. He is a graduate of the Army Management Staff College, class 97-2, Certified level III, Army Acquisition Corps, and undergraduate studies in EE.

CHRISTOPHER T. ALBERT has 10 years of experience in the design, testing, and evaluation of shipboard machinery isolation systems. He designs shipboard automation systems for the U.S. Navy. He holds a B.S. degree in Electrical Engineering from Virginia Tech and a Master of Engineering Management from the George Washington University.

EUGENIO V. ARIAS is a Senior Information Operations planner with the Northern Virginia Operations Center of Syracuse Research Corporation. He is a retired United States Air Force Lieutenant Colonel and has served in the areas of Special Operations, Special Technical Operations, and Acquisition Logistics.

MICHAEL ARMEL is a recent engineering graduate from Penn State University. He is UNIX systems engineer and information security analyst for Lockheed Martin, Management & Data Systems.

EUPHRASIE ASSO-ATAYI is an Internal Information System Auditor at GEICO Corporation. Previously, she has served as an External Information System Auditor for various U.S. government agencies. She also has had Financial Audit experience with nonprofit organizations as well as state government agencies.

LINUS BAKER is an Information Assurance Analyst for Syracuse Research Corporation. He is a veteran of the United States Army where he served as a Military Intelligence Analyst. He holds a B.S. in Computer Science from Brewton-Parker College, and has five years experience in information systems security.

SCOTT BATCHELDER is a technology teacher at Stone Bridge High School and President of Ramsco, Inc. He holds a B.S.Ed. from George Mason University. His graduate work was completed at Stayer University and George Washington University.

JOHN R. BENTZ is a retired U.S. Navy Captain who served 28 years as a Naval Intelligence Officer and now works for a major defense contractor in the Washington, D.C., area. During his naval career he was involved in planning many naval operations that included heavy emphasis on electronic warfare.

CHERYL BILLINGSLEY has a B.S. in Information Systems from Strayer University. Ms. Billingsley is currently a Senior Systems Security Engineer with Mitre Corp.