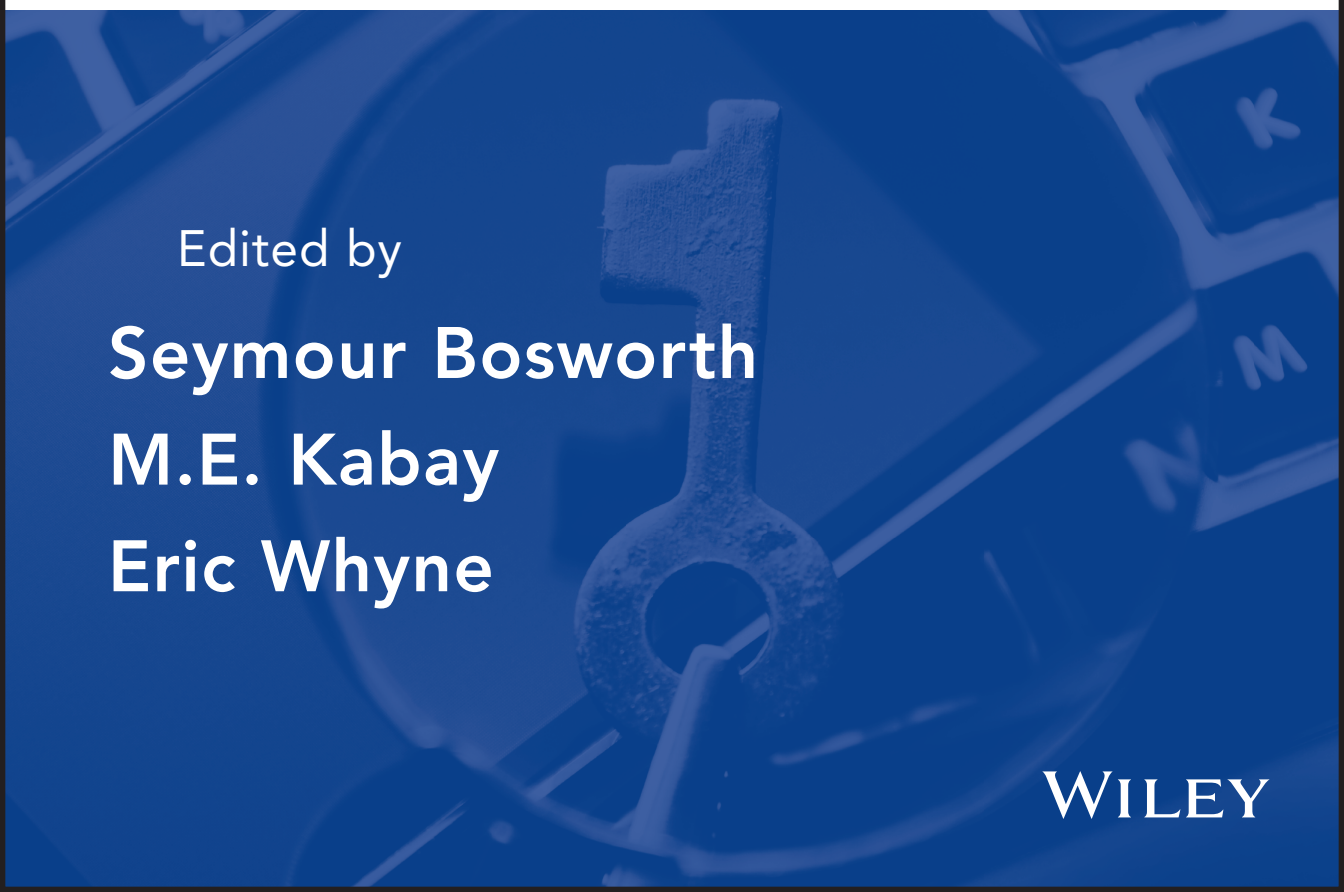
Sixth Edition

COMPUTER SECURITY HANDBOOK



Edited by

Seymour Bosworth

M.E. Kabay

Eric Whyne

WILEY

COMPUTER SECURITY HANDBOOK

COMPUTER SECURITY HANDBOOK

Sixth Edition

Volume 1

Edited by

SEYMOUR BOSWORTH

MICHEL E. KABAY

ERIC WHYNE

WILEY

Cover image: ©iStockphoto.com/Jimmy Anderson
Cover design: Wiley

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Previous Edition: Computer Security Handbook, Fifth Edition. Copyright © 2009 by John Wiley & Sons, Inc. All Rights Reserved. Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data

Computer security handbook / [edited by] Seymour Bosworth, Michel E. Kabay, Eric Whyne. – Sixth edition.
volumes cm
Includes index.
ISBN 978-1-118-13410-8 (vol. 1 : pbk.) – ISBN 978-1-118-13411-5 (vol. 2 : pbk.) – ISBN 978-1-118-12706-3 (2 volume set : pbk.); ISBN 978-1-118-85174-6 (ebk); ISBN 978-1-118-85179-1 (ebk) 1. Electronic data processing departments–Security measures. I. Bosworth, Seymour. II. Kabay, Michel E. III. Whyne, Eric, 1981–
HF5548.37.C64 2014
658.4′78–dc23

2013041083

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

CONTENTS

PREFACE

Computers are an integral part of our economic, social, professional, governmental, and military infrastructures. They have become necessities in virtually every area of modern life, but their vulnerability is of increasing concern. Computer-based systems are constantly under threats of inadvertent error and acts of nature, as well as those attributable to unethical, immoral, and criminal activities. It is the purpose of *The Computer Security Handbook* to provide guidance in recognizing these threats, eliminating them where possible and, if not, then reducing any losses attributable to them.

The Handbook will be most valuable to those directly responsible for computer, network, or information security, as well as those who must design, install, and maintain secure systems. It will be equally important to those managers whose operating functions can be affected by breaches in security and to those executives who are responsible for protecting the assets that have been entrusted to them.

With the advent of desktop, laptop, and handheld computers, and with the vast international networks that interconnect them, the nature and extent of threats to computer security have grown almost beyond measure. In order to encompass this unprecedented expansion, *The Computer Security Handbook* has grown apace.

When the first edition of the *Handbook* was published, its entire focus was on mainframe computers, the only type then in widespread use. The second edition recognized the advent of small computers, while the third edition placed increased emphasis on PCs and networks.

Edition	Publication Date	Chapters	Text Pages
First	1973	12	162
Second	1988	19	383
Third	1995	23	571
Fourth	2002	54	1,184
Fifth	2009	77	2,040
Sixth	2014	75	2,224

The fourth edition of *The Computer Security Handbook* gave almost equal attention to mainframes and microcomputers, requiring more than twice the number of chapters and pages as the third.

The fifth edition was as great a step forward as the fourth. With 77 chapters and the work of 86 authors, we increased coverage in both breadth and depth. In this sixth edition, we updated all chapters while continuing to cover all 10 domains of the Common Body of Knowledge, as defined by the International Information Systems Security Certification Consortium (ISC)[2]:

1. Security Management Practices: Chapters 10, 12, 13, 14, 15, 19, 10, 31, 43, 44, 45, 46, 47, 48, 49, 50, 51, 54, 55, 62, 63, 64, 65, 66, 67, 68, 74, 75
2. Security Architecture and Models: Chapters 1, 2, 3, 8, 9, 24, 26, 27, 51
3. Access Control Systems and Methodology: Chapters 15, 19, 28, 29, 32
4. Application Development Security: Chapters 13, 19, 21, 30, 38, 39, 52, 53
5. Operations Security: Chapters 13, 14, 15, 19, 21, 24, 36, 40, 47, 53, 57
6. Physical Security: Chapters 4, 13, 15, 19, 22, 23, 28, 29
7. Cryptography: Chapters 7, 32, 37, 42
8. Telecomm, Networks, and Internet Security: Chapters 4, 5, 6, 13, 14, 15, 16, 17, 18, 20, 21, 24, 25, 26, 27, 30, 31, 32, 33, 34, 35, 41, 48
9. Business Continuity Planning: Chapters 22, 23, 56, 57, 58, 59, 60
10. Law, Investigations, and Ethics: Chapters 11, 12, 13, 31, 42, 61

We have continued our practice from the fourth and fifth editions of inviting a security luminary to write the final chapter, "The Future of Information Assurance." We are pleased to include this stellar contribution from Jeremy A. Hansen.

SEYMOUR BOSWORTH
Editor-in-Chief
February 2014

ACKNOWLEDGMENTS

Seymour Bosworth, Editor-in-Chief. I would like to give grateful recognition to Arthur Hutt and Douglas Hoyt, my coeditors of the first, second, and third editions of this *Handbook.* Although both Art and Doug are deceased, their commitment and their competence remain as constant reminders that nothing less than excellence is acceptable. Mich Kabay, my coeditor from the fourth and fifth editions, and Eric Whyne, our fellow editor from the fifth and now sixth editions, continue in that tradition. I would not have wanted to undertake this project without them.

Thanks are also due to our colleagues at John Wiley & Sons: Tim Burgard as former Acquisitions Editor, Helen Cho as Editorial Program Coordinator, Sheck Cho as Executive Editor, Kimberly Kappmeyer as Production Editor, Natasha Andrews as Senior Production Editor, and Darice Moore as Copyeditor. All have performed their duties in an exemplary manner and with unfailing kindness, courtesy, and professionalism.

M. E. Kabay, Technical Editor. I want to thank my beloved wife, Deborah Black, light of my life, for her support and understanding over the years that this project has taken away from our time together. I am also grateful to the authors who have selflessly contributed so much to updating the material presented in this text.

Eric Whyne, Administrative Editor. An undertaking as big as pulling together this handbook would not be possible without my wife Lindsay and the love and support she gives to me and to our son Colton. I'd also like to thank the friends and mentors that have helped me most in my career: Mich and Sy, Tom Aldrich, Tom Payne, Frank Vanecek, and my parents Len and Terri. Any successful undertakings I've had, including this book, have been from listening to the advice they've given and aspiring to internalize the virtues that they exemplify. The authors who have contributed to this book also deserve many thanks for sharing their experience and wisdom. It is something for which I, myself, and the readers are extremely grateful.

ABOUT THE EDITORS

Seymour Bosworth, M.S., CDP (email: sybosworth55@gmail.com) is president of S. Bosworth & Associates, Plainview, New York, a management consulting firm specializing in computing applications for banking, commerce, and industry. Since 1972, he has been a contributing editor for all six editions of the *Computer Security Handbook,* and for several editions has been Editor-in-Chief. He has written many articles and lectured extensively about computer security and other technical and managerial subjects. He has been responsible for the design and manufacture, systems analysis, programming, and operations, of both digital and analog computers. For his technical contributions, including an error-computing calibrator, a programming aid, and an analog-to-digital converter, he has been granted a number of patents, and is working on several others.

Bosworth is a former president and CEO of Computer Corporation of America, manufacturers of computers for scientific and engineering applications; president of Abbey Electronics Corporation, manufacturers of precision electronic instruments and digital devices; and president of Alpha Data Processing Corporation, a general-purpose computer service bureau. As a vice president at Bankers Trust Company, he had overall responsibility for computer operations, including security concerns.

For more than 20 years, Bosworth was an adjunct associate professor of management at the Information Technologies Institute of New York University, where he lectured on computer security and related disciplines. He has conducted many seminars and training sessions for the Battelle Institute, New York University, the Negotiation Institute, the American Management Association, and other prestigious organizations. For many years he served as arbitrator, chief arbitrator, and panelist for the American Arbitration Association. He holds a master's degree from the Graduate School of Business of Columbia University and a Certificate in Data Processing from the Data Processing Management Association.

M. E. Kabay, Ph.D., CISSP-ISSMP (email: mekabay@gmail.com) has been programming since 1966. In 1976, he received his Ph.D. from Dartmouth College in applied statistics and invertebrate zoology. After joining a compiler and relational database team in 1979, he worked for Hewlett-Packard (Canada) Ltd. from 1980 through 1983 as an HP3000 operating system performance specialist and then ran operations at a large service bureau in Montréal in the mid-1980s before founding his own operations management consultancy. From 1986 to 1996, he was an adjunct instructor in the John Abbott College professional programs in programming and in technical support. He was director of education for the National Computer Security Association from 1991 to the end of 1999 and was security leader for the INFOSEC Group of AtomicTangerine, Inc., from January 2000 to June 2001. In July 2001, he joined the

faculty at Norwich University as associate professor of computer information systems in the School of Business and Management. In January 2002, he took on additional duties as the director of the graduate program in information assurance in the School of Graduate and Continuing Studies at Norwich, where he was also chief technical officer for several years. He returned to full-time teaching in the School of Business and Management in 2009 and was promoted to professor of computer information systems in 2011. He serves as associate director of the Norwich University Center for Advanced Computing and Digital Forensics.

Kabay was inducted into the Information Systems Security Association Hall of Fame in 2004. He has published more than 1,500 articles in operations management and security in several trade journals since 1986. He wrote two columns a week for *Network World Security Strategies* between 2000 and 2011; archives are at www.mekabay.com/nwss. For the last three editions, Kabay has been Technical Editor of the *Computer Security Handbook.* He also has a Website with freely available teaching materials and papers at www.mekabay.com.

Eric Whyne (email: ericwhyne@gmail.com), administrative editor of the *Computer Security Handbook*, is a technical manager and engineer at Data Tactics Corporation where he develops solutions that benefit national security, currently managing and working on several DARPA-funded big data and data science projects. Prior to this position, he was employed by Exelis Corp. and managed the Joint Improvised Explosive Device Defeat Organization (JIEDDO) Counter-IED Operations Integration Center (COIC) Systems Integration Laboratory (SIL), which consisted of engineers and analysts tasked to develop, deploy, and maintain global software and systems designed to provide intelligence to help predict and prevent explosive devices in Iraq and Afghanistan. Previously, he worked as an engineer with Pennsylvania State University Applied Research Labs (PSU ARL) researching the development and use of immersive visualization systems, geospatial information systems, visual data mining, and deploying touch interfaces in operational environments.

Prior to his industry experience, Whyne spent nine years on active duty in the United States Marine Corps (USMC) in ground combat units, starting as enlisted and attaining the rank of captain. His accomplishments in the Marine Corps include two meritorious promotions and a Navy Commendation Medal with Valor distinction for actions in combat. During his time in the military, he worked in the fields of signals intelligence and communications and served as an advisor to the Iraqi Army. Since 2005, he has been the coordinating editor for the 5th and 6th editions of the *Computer Security Handbook*. He contributes to several open source projects, serves as an invited technical expert in the W3C HTML5 working group, and is a member of the AFCEA Technology Committee.

Whyne attended Norwich University and graduated magna cum laude with a B.S. in computer science and minor degrees in mathematics, information assurance, and engineering.

ABOUT THE CONTRIBUTORS

Wendy Adams Carr currently works for the U.S. Army Corps of Engineers as a member of the Computer Incident Response Team (CIRT). Prior to this she performed as an Information Assurance Security Engineer with Booz Allen & Hamilton, where she supported a Department of Defense client in developing and maintaining DITSCAP and DIACAP-based certification and accreditation of complex, large-scale Information Systems. She is retired from the U.S. Army. She is also an active member of Infragard.

Mani Akella, a director (technology), has been actively working with information-security architectures and identity protection for Consultantgurus and its clients. An industry professional for 20 years, he has worked with hardware, software, networking, and all the associated technologies that service information in all of its incarnations and aspects. Over the years, he has developed a particular affinity for international data law and understanding people and why they do what they do (or do not). He firmly believes that the best law and policy is that which understands and accounts for cross-cultural differences, and works with an understanding of culture and societal influences. To that end, he has been actively working with all his clients and business acquaintances to improve security policies and make them more people-friendly: His experience has been that the best policy is that which works with, instead of being antagonistic to, the end user.

Rebecca Gurley Bace is the president/CEO of Infidel, Inc., a strategic consulting practice headquartered in Scotts Valley, California. She is also a venture consultant for Palo Alto–based Trident Capital, where she is credited with building Trident's investment portfolio of security product and service firms. Her areas of expertise include intrusion detection and prevention, vulnerability analysis and mitigation, and the technical transfer of information-security research results to the commercial product realm. Prior to transitioning to the commercial world, she worked in the public sector, first at the National Security Agency, where she led the Intrusion Detection research program, then at the Computing Division of the Los Alamos National Laboratory, where she served as deputy security officer. Her publishing credits include two books, an NIST Special Publication on intrusion detection and prevention, and numerous articles on information-security technology topics.

Susan Baumes, MS, CISSP, is an information-security professional working in the financial services industry. In her current role, she works across the enterprise to develop information-security awareness and is responsible for application security. Her role also extends to policy development, compliance, and audit. She has 11 years'

experience in application development, systems and network administration, database management, and information security. Previously, she worked in a number of different sectors, including government (federal and state), academia, and retail.

Kurt Baumgarten, CISA, is vice president of information security and a partner at Peritus Security Partners, LLC, a leader in providing compliance-driven information security solutions. He is also a lecturer, consultant, and the developer of the DDIPS intrusion prevention technology as well as a pioneer in using best practices frameworks for the improvement of information technology security programs and management systems. He has authored multiple articles about the business benefits of sound information technology and information assurance practices, and assists businesses and government agencies in defining strategic plans that enhance IT and IA as positive value chain modifiers. He holds both a master's of science in information assurance and an M.B.A. with a concentration in e-commerce, and serves as an adjunct professor of information assurance. He has more than 20 years of experience in IT infrastructure and information security and is an active member of ISSA, ISACA, ISSSP, and the MIT Enterprise Forum. He periodically acts as an interim Director within external organizations in order to facilitate strategic operational changes in IT and information security.

Kevin Beets has been a research scientist with McAfee for over nine years. His work has concentrated on vulnerability, exploit and malware analysis, and documentation for the Foundstone and McAfee Labs teams. Prior to working with McAfee, he architected private LANS as well as built, monitored, and supported CheckPoint and PIX firewalls and RealSecure IDS systems.

Matt Bishop is a professor in the Department of Computer Science at the University of California at Davis and a codirector of the Computer Security Laboratory. His main research area is the analysis of vulnerabilities in computer systems, especially their origin, detection, and remediation. He also studies network security, policy modeling, and electronic voting. His textbook, *Computer Security: Art and Science*, is used widely in advanced undergraduate and graduate courses. He received his Ph.D. in computer science from Purdue University, where he specialized in computer security, in 1984.

Kip Boyle is the chief information-security officer of PEMCO Insurance, a $350 million property, casualty, and life insurance company serving the Pacific Northwest. Prior to joining PEMCO Insurance, he held such positions as chief security officer for a $50 million national credit card transaction processor and technology service provider; authentication and encryption product manager for Cable & Wireless America; senior security architect for Digital Island, Inc.; and a senior consultant in the Information Security Group at Stanford Research Institute (SRI) Consulting. He has also held director-level positions in information systems and network security for the U.S. Air Force. He is a Certified Information System Security Professional and Certified Information Security Manager. He holds a bachelor's of science in computer information systems from the University of Tampa (where he was an Air Force ROTC Distinguished Graduate) and a master's of science in management from Troy State University.

Jennifer Bradley is a member of the first Master of Science in Information Assurance graduating class at Norwich University. She is the primary Systems and Security Consultant for Indiana Networking in Lafayette, Indiana, and has served as both a

network and systems administrator in higher education and private consulting. She has almost 15 years' experience as a programmer and instructor of Web technologies, with additional interests in data backup, virtualization, authentication/identification, monitoring, desktop and server deployment, and incident response. At present she serves as an independent consultant. She has previously worked as a tester for quality and performance projects for Google, Inc., and as a collegiate adjunct instructor in computer technologies. She received a bachelor's of science in Industrial and Computer Technology from Purdue University.

Timothy Braithwaite has more than 30 years of hands-on experience in all aspects of automated information processing and communications. He is currently the deputy director of strategic programs at the Center for Information Assurance of Titan Corporation. Before joining Titan, he managed most aspects of information technology, including data and communications centers, software development projects, strategic planning and budget organizations, system security programs, and quality improvement initiatives. His pioneering work in computer systems and communications security while with the Department of Defense resulted in his selection to be the first systems security officer for the Social Security Administration (SSA) in 1980. After developing security policy and establishing a nationwide network of regional security officers, he directed the risk assessment of all payment systems for the agency. In 1982, he assumed the duties of deputy director, systems planning and control of the SSA, where he performed substantive reviews of all major acquisitions for the associate commissioner for systems and, through a facilitation process, personally led the development of the first Strategic Systems Plan for the administration. In 1984, he became director of information and communication services for the Bureau of Alcohol, Tobacco, and Firearms at the Department of Treasury. In the private sector, he worked in senior technical and business development positions for SAGE Federal Systems, a software development company; Validity Corporation, a testing and independent validation and verification company; and J.G. Van Dyke & Associates, where he was director, Y2K testing services. He was recruited to join Titan Corporation in December 1999 to assist in establishing and growing the company's Information Assurance practice.

Dr. Paul Brusil founded Strategic Management Directions, a security and enterprise management consultancy in Beverly, Massachusetts. He has been working with various industry and government sectors, including healthcare, telecommunications, and middleware to improve the specification, implementation, and use of trustworthy, quality, security-related products and systems. He supported strategic planning that led to the National Information Assurance Partnership and other industry forums created to understand, promote, and use the Common Criteria to develop security and assurance requirements and to evaluate products. He has organized, convened, and chaired several national workshops, conferences, and international symposia pertinent to management and security. Through these and other efforts to stimulate awareness and cooperation among competing market forces, he spearheaded industry's development of the initial open, secure, convergent, standards-based network and enterprise management solutions. While at the MITRE Corp, he led research and development critical to the commercialization of the world's first LAN solutions. Earlier, at Harvard, he pioneered research leading to noninvasive diagnosis of cardiopulmonary dysfunction. He is a Senior Member of the IEEE, a member of the Editorial Advisory Board of the *Journal of Network and Systems Management* (JNSM), has been senior technical editor for JNSM, is the guest editor for all JNSM's Special Issues on Security and Management,

and is a lead instructor for the adjunct faculty supporting the master's of science in information assurance degree program at Norwich University. He has authored over 100 papers and book chapters. He graduated from Harvard University with a joint degree in Engineering and Medicine.

Michael Buglewicz is employed at National Security Technologies as a section manager whose team provides technology and communications solutions to various government agencies. He spent 17 years at Microsoft in various roles in services and business management. Prior to Microsoft, he was involved with building some of the first Internet ecommerce and banking solutions while at First Data Corporation; he also spent ten years in law enforcement. In addition to his contributions to *The Computer Security Handbook*, he was a contributing author to *The Encyclopedia of Information Assurance* and, most recently, contributed to the book *Cloud Migration* by Tobias Hollwarth.

Dr. Joseph R. Bumblis is currently a research specialist with the Institute of Electrical and Electronic Engineers (IEEE) Twin Cities (TC) Section's Phoenix Project, where he conducts research and engineering projects in the areas of sensors, signal processing, and embedded systems design. His expertise includes computer networks, embedded systems with FPGA and SoC codesign, IT systems security, and software engineering methodologies. As an Associate Professor of Computer Engineering at the University of Wisconsin-Stout (UW-Stout), he developed computer engineering curriculum and taught courses in digital design, solid-state devices, embedded systems design, and Verilog programming. Prior to joining UW-Stout, he served as an IT systems architect at BAE Systems and held several adjunct professor positions where he taught software engineering and computer networking courses.

Q. Campbell has worked in the information-security field for over six years. He specializes in information-security threat analysis and education.

Santosh Chokhani is the founder and president of CygnaCom Solutions, Inc., an Entrust company specializing in PKI. He has made numerous contributions to PKI technology and related standards, including trust models, security, and policy and revocation processing. He is the inventor of the PKI Certificate Policy and Certification Practices Statement Framework. His pioneering work in this area led to the Internet RFC that is used as the standard for CP and CPS by governments and industry throughout the world. Before starting CygnaCom, he worked for The MITRE Corporation from 1978 to 1994. At MITRE, he was senior technical manager and managed a variety of technology research, development, and engineering projects in the areas of PKI, computer security, expert systems, image processing, and computer graphics. Chokhani obtained his master's (1971) and Ph.D. (1975) in electrical engineering/computer science from Rutgers University, where he was a Louis Bevior Fellow from 1971 to 1973.

Christopher Christian is a first lieutenant and an aviator in the United States Army. He received a bachelor's degree in Computer Information Systems at Norwich University class of 2005. His primary focus of study was Information Assurance and Security. He worked as an intern for an engineering consulting company for three years. He developed cost/analysis worksheets and floor-plan layouts to maximize workspace efficiency for companies in various industries. He graduated flight school at Fort Rucker, Alabama, where he trained on the H-60 Blackhawk. He serves as a flight

platoon leader in an air assault battalion. He is currently serving in Iraq in support of Operation Iraqi Freedom 08–09.

Chey Cobb, CISSP, began her career in information security while at the National Computer Security Association (now known as TruSecure/ICSA Labs). During her tenure as the NCSA award–winning Webmaster, she realized that Web servers often created security holes in networks and became an outspoken advocate of systems security. Later, while developing secure networks for the Air Force in Florida, her work captured the attention of the U.S. intelligence agencies. She moved to Virginia and began working for the government as the senior technical security advisor on highly classified projects. Ultimately, she went on to manage the security program at an overseas site. Now semiretired, she writes books and articles on computer security and is a frequent speaker at security conferences.

Stephen Cobb, CISSP, is an independent information-security consultant and an adjunct professor of information assurance at Norwich University, Vermont. A graduate of the University of Leeds, his areas of expertise include risk assessment, computer fraud, data privacy, business continuity management, and security awareness and education. A frequent speaker and seminar leader at industry conferences around the world, he is the author of numerous books on security and privacy as well as hundreds of articles. He cofounded several security companies whose products expanded the range of security solutions available to enterprises and government agencies. As a consultant, he has advised some of the world's largest companies on how to maximize the benefits of information technology by minimizing IT risks.

Caleb S. Coggins, MSIA, GSNA, CISSP, CISA, currently works for Sylint in the area of network forensics. Prior to Sylint, he operated in an internal audit and advisory services capacity for a healthcare IT company in Tennessee that focused on revenue and payment cycle management. Previous to that, he served in IT, security, and audit functions at Bridgestone Americas and its subsidiaries for over eight years. During his time working in the Americas and West Africa, he has enjoyed collaborating with management and teammates in identifying practical and effective solutions, while reducing risk to business operations. Prior to Bridgestone, he was the information manager for a private company as well as an information-security consultant to business clients. He holds a B.A. from Willamette University and an M.S. in information assurance from Norwich University.

Bernie Cowens, CISSP, CISA, is chief information-security officer at a Fortune 500 company in the financial services industry. He is an information risk, privacy, and security expert with more than 20 years' experience in industries including defense, high technology, healthcare, financial, and Big Four professional services. He has created, trained, and led a number of computer emergency, forensic investigation, and incident response teams over the years. He has real-world experience responding to attacks, disasters, and failures resulting from a variety of sources, including malicious attackers, criminals, and foreign governments. He has served as an advisor to and a member of national-level panels charged with analyzing cybersystem threats to critical infrastructures, assessing associated risks, and recommending both technical and nontechnical mitigation policies and procedures. He holds a master's degree in management information systems along with undergraduate degrees and certificates in systems management and information processing.

Tim Crothers is an IT manager at 3M IT.

Rob Cryan is chief information-security officer for MAPFRE USA, consisting of seven property and casualty insurance companies in the United States. He has corporate responsibility for all aspects of information security and business continuity. He has worked in both the corporate and the consulting fields, managing and delivering security solutions. His current areas of focus include managing risk in cloud computing and delivering cost-effective risk management derived from larger, often cumbersome models to apply uniform controls across multiple compliance disciplines. He received his B.S. in business administration management from the University of Maine. He is currently pursuing his M.S. in information systems and technology management with a concentration in information assurance and security.

Christopher Dantos is a senior architectural specialist with Computer Science Corporation's Global Security Solutions Group. His areas of expertise include 802.11, VoIP, and Web application security. Prior to joining CSC, he spent 10 years as a security architect with Motorola Inc., including five years in the Motorola Labs Wireless Access Research Center of Excellence. He holds a master's of science degree in information assurance from Norwich University and a bachelor's of science degree in marine engineering from the Maine Maritime Academy.

Scott L. David is executive director of the Law, Technology, and Arts Group at the University of Washington School of Law.

Chris Davis, MBA, CISA, CISSP, CCNP, finds that his role as a cloud security and compliance product manager at VCE enables him to apply his past experiences to the latest in data center computing. He has trained and presented in information security, audit, forensic analysis, hardware security design, auditing, and systems engineering for government, corporate, and university requirements. He has written or contributed to nine books covering multiple security disciplines and teaches as an adjunct professor at Southern Methodist University covering graduate courses in Information Security and Risk Management (EMIS7380) and IT Controls (EMIS7382). His professional career has taken him through Texas Instruments followed by several startup and consulting roles. He holds a bachelor's degree in nuclear engineering technologies from Thomas Edison State College and a master's in business from the University of Texas McCombs School of Business at Austin. He served eight years in the U.S. Naval Submarine Fleet onboard the special projects Submarine NR-1 and the ballistic missile submarine USS Nebraska.

Seth Finkelstein is a professional programmer with degrees in Mathematics and in Physics from MIT. He cofounded the Censorware Project, an anti-censorware advocacy group. In 1998, his efforts evaluating the sites blocked by the library's Internet policy in Loudoun County, Virginia, helped the American Civil Liberties Union win a federal lawsuit challenging the policy. In 2001, he received a Pioneer of the Electronic Frontier Award from the Electronic Frontier Foundation for his groundbreaking work in analyzing content-blocking software. In 2003, he was primarily responsible for winning a temporary exemption in the Digital Millennium Copyright Act allowing for the analysis of censorware.

Eric Fisher is a systems architecture and network security engineer for Penn State University's Applied Research Laboratories and is currently a master's candidate

in the field of information security and forensics. Eric has extensive experience designing and implementing high performance and redundant compute systems for the Department of Defense and the IC at large. His areas of expertise are designing and implementing secure and scalable information systems, and the networks that connect them. Before joining Penn State, he worked for the Raytheon Corporation as a *nix/Windows/Network administrator where he managed large-scale high-availability clusters.

Robert Gezelter, CDP, has over 33 years of experience in computing, starting with programming scientific/technical problems. Shortly thereafter, his focus shifted to operating systems, networks, security, and related matters, where he has 32 years of experience in systems architecture, programming, and management. He has worked extensively in systems architecture, security, internals, and networks, ranging from high-level strategic issues to the low-level specification, design, and implementation of device protocols and embedded firmware. He is an alumnus of the IEEE Computer Society's Distinguished Visitor Program for North America, having been appointed to a three-year term in 2004. His appointment included many presentations at Computer Society chapters throughout North America. He has published numerous articles, appearing in *Hardcopy, Computer Purchasing Update, Network Computing, Open Systems Today, Digital Systems Journal,* and *Network World*. He is a frequent presenter at conference sessions on operating systems, languages, security, networks, and related topics at local, regional, national, and international conferences, speaking for DECUS, Encompass, IEEE, ISSA, ISACA, and others. He previously authored the mobile code and Internet-related chapters for the 4th edition of this *Handbook* (2002) as well as the "Internet Security" chapters of the 3rd edition (1995) and its supplement (1997). He is a graduate of New York University with B.A. (1981) and M.S. (1983) degrees in computer science. He founded his consulting practice in 1978, working with clients both locally and internationally. He maintains his offices in Flushing, New York. He may be contacted via his firm's Website at www.rlgsc.com.

Dr. Anup K. Ghosh is president and chief executive of Secure Command, LLC, a security software start-up developing next-generation Internet security products for corporate networks. He also holds a position as research professor at George Mason University. He was previously senior scientist and program Manager in the Advanced Technology Office of the Defense Advanced Research Projects Agency (DARPA), where he managed an extensive portfolio of information assurance and information operations programs. He previously served in executive management as Vice President of Research at Cigital, Inc. He has served as principal investigator on contracts from DARPA, NSA, and NIST's Advanced Technology Program and has written more than 40 peer-reviewed conference and journal articles. He is also author of three books on computer network defense, serves on the editorial board of *IEEE Security and Privacy Magazine*, and has been guest editor for *IEEE Software* and *IEEE Journal on Selected Areas in Communications*. He is a Senior Member of the IEEE. For his contributions to the Department of Defense's information assurance, he was awarded the Frank B. Rowlett Trophy for Individual Contributions by the National Security Agency in November 2005, a federal government–wide award. He was also awarded the Office of the Secretary of Defense Medal for Exceptional Public Service for his contributions while at DARPA. In 2005, Worcester Polytechnic Institute awarded him its Hobart Newell Award for Outstanding Contributions to the Electrical and Computer Engineering Profession. He has previously been awarded the IEEE's Millennium Medal for Outstanding Contributions to E-Commerce Security. He completed his Ph.D. and

master's of science in electrical engineering at the University of Virginia and his bachelor's of science in electrical engineering at Worcester Polytechnic Institute.

Donald Glass, CISA, CISSP, has over 15 years of experience in the IT Auditing and Information Security fields. He is the current director of IT audit for Kerzner International. Author of several information security and IT audit articles, he is recognized as a leader in the IT audit field and information security.

Robert Guess, CISSP, NSA-IAM, NSA-IEM, is a senior security engineer at a Fortune 500 organization and an Associate Professor of Information Systems Technology. He possesses an M.S. in information assurance and has over a dozen industry certifications, including the Certified Information Systems Security Practitioner (CISSP), National Security Agency INFOSEC Assessment Methodologist (NSA-IAM), and National Security Agency INFOSEC Evaluation Methodologist (NSA-IEM). In addition to his academic experience, his professional experience includes work within the air, space, and defense sectors, serving as primary subject matter expert on a National Science Foundation cybersecurity grant, the development of workforce certification standards for information assurance professionals (DOD 8570.01-m), and periodic work as both an editor and author (e.g., the 5th and 6th editions of *The Computer Security Handbook*, etc.). His work in recent years has focused on penetration testing, incident response, the forensic analysis of digital evidence, virtualization, and cloud computing.

David Gursky, CISA, CISM, CISSP, is an information assurance manager and researcher at Raytheon Integrated Defense Systems working in Crystal City, Virginia. He is principal investigator for behavior-based intrusion detection systems, attribute-based access control, and resource-efficient authentication techniques. He held several senior positions as a Department of Defense contractor supporting information assurance programs and has over 30 years' experience in information technology and information security. He has conducted numerous security audits for PriceWaterhouse and Coopers. He has a bachelor's of science degree in business management from Southern New Hampshire University, a master's of science degree from Norwich University, and an M.B.A. from Northeastern University. In addition, he holds a CISA, CISM, and CISSP certifications. He lives in Northern Virginia and is an active member of $(ISC)^2$ and ISACA.

Jennifer Hadley is a member of the first master's of science in information assurance graduating class at Norwich University. She is the primary systems and security consultant for Indiana Networking in Lafayette, Indiana, and has served as both a network and systems administrator in higher education and private consulting. She has almost 10 years' experience as a programmer and instructor of Web technologies with additional interests in data backup, virtualization, authentication/identification, monitoring, desktop and server deployment, and incident response. At present, she serves as a technology consultant for Axcell Technologies, Inc. Previously she worked as a tester for quality and performance projects for Google, Inc., and as a collegiate adjunct instructor in computer technologies. She received a bachelor's of science degree in industrial and computer technology from Purdue University.

Carl Hallberg, CISSP, has been a UNIX systems administrator for years as well as an information-security consultant. He has also written training courses for subjects including firewalls, VPNs, and home network security. He has a bachelor's degree in

psychology. Currently, he is a senior member of an incident response team for a major U.S. financial institution.

Jeremy A. Hansen is an information-security and cryptography educator and researcher.

David Harley, CITP, FBCS, CISSP, is CEO of Small Blue-Green World, COO of AVIEN, and ESET Senior Research Fellow, specializing in antimalware research and security/technical authoring and editing in a number of areas. His books include *Viruses Revealed* and *The AVIEN Malware Defense Guide*. Previously, he managed the UK National Health Service's Threat Assessment Centre, and before that he served as security analyst for the Imperial Cancer Research Fund (now Cancer Research UK). His academic background is in social sciences and computer science, and he is a fellow of the BCS Institute (formerly the British Computer Society).

Benjamin S. Hayes is an IT specialist at Travis Software.

Kevin Henry has been involved in computers since 1976, when he was an operator on the largest minicomputer system in Canada. He has since worked in many areas of information technology, including computer programming, systems analysis, and information technology audit. He was asked to become director of security based on the evidence of his audits and involvement in promoting secure IT operations. Following 20 years in the telecommunications field, he moved to a senior auditor position with the State of Oregon, where he was a member of the Governor's IT Security Subcommittee and performed audits on courts and court-related IT systems. He has extensive experience in risk management and business continuity and disaster recovery planning. He frequently presents papers at industry events and conferences and is on the preferred speakers list for nearly every major security conference. Since joining $(ISC)^2$ as their first full-time program manager in 2002, he has been responsible for research and development of new certifications, courseware, and development of educational programs and instructors. He has also been providing support services and consulting for organizations that require in-depth risk analysis and assistance with specific security-related challenges. This has led to numerous consulting engagements in the Middle East and Asia for large telecommunications firms, government departments, and commercial enterprises.

Don Holden, CISSP, ISSMP, is a principal consultant with Concordant specializing in information security. He has more than 20 years of management experience in information systems, security, encryption, business continuity, and disaster recovery planning in both industry and government. Previously he was a technology leader for RedSiren Technologies (formerly SRI Consulting). His achievements include leading a cyberinsurance joint venture project, developing privacy and encryption policies for major financial institutions, and recommending standards-based information technology security policies for a federal financial regulator. Holden is an adjunct professor for the Norwich University's master's of science in information assurance. He received an M.B.A. from Wharton and is a Certified Information System Security Professional and Information System Security Management Professional.

Dr. John D. Howard is a former Air Force engineer and test pilot who currently works in the Security and Networking Research Group at the Sandia National Laboratories, Livermore, California. His projects include development of the SecureLink software for

automatic encryption of network connections. He has extensive experience in systems development, including an aircraft–ground collision avoidance system for which he holds a patent. He is a graduate of the Air Force Academy, has master's degrees in both aeronautical engineering and political science, and has a Ph.D. in engineering and public policy from Carnegie Mellon University.

Arthur E. Hutt, CCEP. The late Arthur E. Hutt was an information systems consultant with extensive experience in banking, industry, and government. He served as a contributing editor to the 1st, 2nd, and 3rd editions of *The Computer Security Handbook*. He was a principal of PAGE Assured Systems, Inc., a consulting group specializing in security and control of information systems and contingency/disaster recovery planning. He was a senior information systems executive for several major banks active in domestic and international banking. His innovative and pioneering development of online banking systems received international recognition. He was also noted for his contributions to computer security and to information systems planning for municipal government. He was on the faculty of the City University of New York and served as a consultant to CUNY on curriculum and on data processing management. He also served on the mayor's technical advisory panel for the City of New York. He was active in development of national and international technical standards, via ANSI and ISO, for the banking industry.

John B. Ippolito, CISSP, PMP, is director of information assurance services for the Allied Technology Group, Inc. He has more than 35 years of IT experience including "hands-on" experience with legacy mainframes, PCs, and virtual systems. He has supported government-wide standards efforts and coauthored NIST IT security training guidelines. He has a broad range of IT experience and is currently supporting federal agencies in the development of information assurance and privacy programs and the secure introduction of new technologies such as cloud-based systems and "bring your own device" into the business environment.

Robert V. Jacobson, CPP, CISSP. The late Robert V. Jacobson was the president of International Security Technology, Inc., a New York City–based risk-management consulting firm. He founded IST in 1978 to develop and apply superior risk-management systems. Current and past government and industry clients are located in the United States, Europe, Africa, Asia, and the Middle East. He pioneered many of the basic computer security concepts now in general use. He served as the first information system security officer at Chemical Bank, now known as J P Morgan Chase. He was a frequent lecturer and had written numerous technical articles. He held B.S. and M.S. degrees from Yale University, and was a Certified Information Systems Security Professional. He was also a Certified Protection Professional of the American Society for Industrial Security. He was a member of the National Fire Protection Association and the Information Systems Security Association. In 1991, he received the Fitzgerald Memorial Award for Excellence in Security from the New York Chapter of the ISSA.

David J. Johnson is an information-security architect with a Fortune 500 financial services company where he provides enterprise guidance and solutions on topics such as cloud computing security, data protection technologies, and biometric authentication. His prior experience includes information-security analysis, advising business and IT management and staff on security risk, and development of policies and

procedures for a Fortune 1000 company. He also has experience designing, developing, and maintaining electronic commerce (EC/EDI) infrastructure and data transfers for a national financial services company. He holds a B.S. in business administration from Oregon State University, an M.S. in information assurance from Norwich University, and multiple information-security certifications from $(ISC)^2$, ISACA, and the Cloud Security Alliance.

Henry L. Judy is of counsel to Kirkpatrick & Lockhart, a national U.S. law firm. He advises clients on a wide range of corporate and financial law matters as well as federal and state securities, legislative and regulatory matters, with a particular emphasis on financial institutions, housing finance, and technology law. He is recognized for his work on the jurisdiction and dispute resolution issues of electronic commerce. He is a graduate of Georgetown University (J.D. and A.B.).

Sean Kelley is the vice president of technology services at Evolvent Technologies in Herndon, Virginia. He is a retired Naval Officer with over 15 years of information assurance experience. Sean Kelley has received an M.A. in computer resource and information management from Webster University and an M.S. in information technology management (information assurance core competency) from the Naval Postgraduate School (NPS) in Monterey, California. He concentrated his studies on computer and network security by taking classes through the NPS Center for INFOSEC Studies and Research (NPS CISR), the world's foremost center for military research and education in information assurance (IA), defensive information warfare, and computer and network security. During his tenure at NPS, he received several certifications from the Committee of National Security Systems (CNSS), which operates under NSA. He is a Certified Information Systems Security Professional (CISSP), and is also a Project Management Professional (PMP). He has been responsible for information systems at several high-level offices in Washington, DC, and in the operational setting.

David M. Kennedy, CISSP, is TruSecure Corporation's chief of research. He directs the Research Group to provide expert services to TruSecure Corporation members, clients, and staff. He supervises the Information Security Reconnaissance (IS/R) team, which collects security-relevant information, both above- and underground in TruSecure Corporation's IS/R data collection. IS/R provides biweekly and special topic reports to IS/R subscribers. He is a retired U.S. Army Military Police officer. In his last tour of duty, he was responsible for enterprise security of five LANs with Internet access and over 3,000 personal computers and workstations. He holds a B.S. in forensic science.

Dr. Gary C. Kessler, CISSP, CCE, is an associate professor of Homeland Security at Embry-Riddle Aeronautical University in Daytona Beach, Florida, specializing in cybersecurity. He is a member of the North Florida Internet Crimes against Children (ICAC) Task Force and an adjunct faculty member at Edith Cowan University in Perth, Western Australia. From 2011 to 2012, he was the program director of the M.S. in Information Assurance program at Norwich University in Northfield, Vermont; from 2000 to 2010, he was an associate professor at Champlain College in Burlington, Vermont, where he designed and directed undergraduate and graduate programs related to information security and digital forensics. He is a Certified Information Systems Security Professional (CISSP), Certified Computer Examiner (CCE), and on the board of directors of the Consortium of Digital Forensic Specialists (CDFS). He holds a B.A.

in mathematics, an M.S. in computer science, and a Ph.D. in computing technology in education. He is the coauthor of two professional texts and over 70 articles and papers, a frequent speaker at industry events, and immediate past editor-in-chief of the *Journal of Digital Forensics, Security, and Law*. More information about him can be found at www.garykessler.net.

Dr. Minjeong Kim is associate professor of Journalism and Technical Communication at the Colorado State University. Her areas of expertise include communication law and policy, copyright law, and digital media. Her research has been published in scholarly journals, including *Communication Law and Policy*, the *Journal of the Copyright Society of the U.S.A.*, the *Journal of Computer-Mediated Communication*, and *Telecommunications Policy*. She completed her M.A. and Ph.D. from the School of Journalism and Mass Communication at the University of North Carolina at Chapel Hill. Before joining the CSU faculty in Fall 2008, she was an assistant professor at Hawaii Pacific University in Honolulu.

David A. Land served in the U.S. Army as a Counterintelligence Special Agent. With David Christie, he developed and hosted the first Department of Defense Computer Crimes Conference. Since then he has investigated espionage cases for both the Army and the Department of Energy. He serves as the information technology coordinator for Anniston City Schools in Alabama and as an adjunct professor for Norwich University, his alma mater.

David T. Lang joined the U.S. Civil Service on August 15, 2011. He has more than 30 years of experience in technical program management, counterespionage, antiterrorism, security, training, risk management, and law enforcement in private industry and the military. Before assuming his current position as director of the DCIN-TS PMO, he was the chief of enterprise architecture and security for the DCIN-TS PMO. His industry positions included director of federal security, director of information assurance and forensics, director of digital forensics, and director of external training. His military assignments included nearly a decade as a Special Agent for the Air Force Office of Special Investigations (AFOSI) and over a decade in special weapons.

Dr. David R. Lease is the Chief Solution Architect at Computer Sciences Corporation. He has over 30 years of technical and management experience in the information technology, security, telecommunications, and consulting industries. His recent projects include a $2 billion security architecture redesign for a federal law enforcement agency and the design and implementation of a secure financial management system for an organization operating in 85 countries. He is a writer and frequent speaker at conferences for organizations in the intelligence community, Department of Defense, civilian federal agencies, as well as commercial and academic organizations. He is also a peer reviewer of technical research for the IEEE Computer Society. Additionally, he is on the faculty of Norwich University and the University of Fairfax, where he teaches graduate-level information assurance courses and supervises doctoral-level research.

Corinne Lefrançois is an information assurance analyst at the National Security Agency. She graduated from Norwich University with a bachelor's of science in business administration and accounting in 2004 and is a current student in Norwich University's master's of science in information assurance program.