Lead Authors and Technical Editors

Craig A. Schiller (CISSP-ISSMP, ISSAP) is the Chief Information Security Officer for Portland State University and President of Hawkeye Security Training, LLC. He is the primary author of the first Generally Accepted System Security Principles. He was a coauthor of several editions of the *Handbook of Information Security Management* and a contributing author to *Data Security Management*. Craig was also a contributor to *Combating Spyware in the Enterprise* (Syngress, ISBN: 1597490644) and *Winternals Defragmentation, Recovery, and Administration Field Guide* (Syngress, ISBN: 1597490792). Craig was the Senior Security Engineer and Coarchitect of NASA's Mission Operations AIS Security Engineering Team. Craig has cofounded two ISSA U.S. regional chapters: the Central Plains Chapter and the Texas Gulf Coast Chapter. He is a member of the Police Reserve Specialists unit of the Hillsboro Police Department in Oregon. He leads the unit's Police-to-Business-High-Tech speakers' initiative and assists with Internet forensics.

Jim Binkley is a senior network engineer and network security researcher at Portland State University (PSU). Jim has over 20 years of TCP/IP experience and 25 years of UNIX operating system experience. Jim teaches graduate-level classes in network security, network management, and UNIX operating systems at PSU. He provides the university with various forms of network monitoring as well as consulting in network design. In the past Jim was involved in the DARPA-funded "secure mobile networks" grant at PSU along with John McHugh. His specialties include wireless networking and network anomaly detection, including the open-source ourmon network monitoring and anomaly detection system. Jim holds a Master of Science in Computer Science from Washington State University.

Contributors

Tony Bradley (CISSP-ISSAP) is the Guide for the Internet/Network Security site on About.com, a part of The New York Times Company. He has written for a variety of other Web sites and publications, including *PC World*, SearchSecurity.com, WindowsNetworking.com, *Smart Computing* magazine, and *Information Security* magazine. Currently a security architect and consultant for a Fortune 100 company, Tony has driven security policies and technologies for antivirus and incident response for Fortune 500 companies, and he has been network administrator and technical support for smaller com-

panies. He is author of *Essential Computer Security: Everyone's Guide to E-mail, Internet, and Wireless Security* (Syngress, ISBN: 1597491144).

Tony is a CISSP (Certified Information Systems Security Professional) and ISSAP (Information Systems Security Architecture Professional). He is Microsoft Certified as an MCSE (Microsoft Certified Systems Engineer) and MCSA (Microsoft Certified Systems Administrator) in Windows 2000 and an MCP (Microsoft Certified Professional) in Windows NT. Tony is recognized by Microsoft as an MVP (Most Valuable Professional) in Windows security.

On his About.com site, Tony has on average over 600,000 page views per month and 25,000 subscribers to his weekly newsletter. He created a 10-part Computer Security 101 Class that has had thousands of participants since its creation and continues to gain popularity through word of mouth. In addition to his Web site and magazine contributions, Tony was also coauthor of *Hacker's Challenge 3* (ISBN: 0072263040) and a contributing author to *Winternals: Defragmentation, Recovery, and Administration Field Guide* (ISBN: 1597490792) and *Combating Spyware in the Enterprise* (ISBN: 1597490644).

Tony wrote Chapter 4.

Michael Cross (MCSE, MCP+I, CNA, Network+) is an Internet Specialist/Computer Forensic Analyst with the Niagara Regional Police Service (NRPS). He performs computer forensic examinations on computers involved in criminal investigation. He also has consulted and assisted in cases dealing with computer-related/Internet crimes. In addition to designing and maintaining the NRPS Web site at www.nrps.com and the NRPS intranet, he has provided support in the areas of programming, hardware, and network administration. As part of an information technology team that provides support to a user base of more than 800 civilian and uniform users, he has a theory that when the users carry guns, you tend to be more motivated in solving their problems.

Michael also owns KnightWare (www.knightware.ca), which provides computer-related services such as Web page design, and Bookworms (www.bookworms.ca), where you can purchase collectibles and other interesting items online. He has been a freelance writer for several years, and he has been published more than three dozen times in numerous books and anthologies. He currently resides in St. Catharines, Ontario, Canada, with his lovely wife, Jennifer, his darling daughter, Sara, and charming son, Jason.

Michael wrote Chapter 11.

Gadi Evron works for the McLean, VA-based vulnerability assessment solution vendor Beyond Security as Security Evangelist and is the chief editor of the security portal SecuriTeam. He is a known leader in the world of Internet security operations, especially regarding botnets and phishing. He is also the operations manager for the Zeroday Emergency Response Team (ZERT) and a renowned expert on corporate security and espionage threats. Previously, Gadi was Internet Security Operations Manager for the Israeli government and the manager and founder of the Israeli government's Computer Emergency Response Team (CERT).

Gadi wrote Chapter 3.

David Harley (BA, CISSP) has written or contributed to over a dozen security books, including *Viruses Revealed* and the forthcoming *AVIEN Malware Defense Guide for the Enterprise*. He is an experienced and well-respected antivirus researcher, and he also holds qualifications in security audit (BS7799 Lead Auditor), ITIL Service Management, and medical informatics. His background includes security analysis for a major medical research charity and managing the Threat Assessment Centre for the U.K.'s National Health Service, specializing in the management of malware and e-mail security. His "Small Blue-Green World" provides consultancy and authoring services to the security industry, and he is a frequent speaker at security conferences.

David cowrote Chapter 5.

Chris Ries is a Security Research Engineer for VigilantMinds Inc., a managed security services provider and professional consulting organization based in Pittsburgh. His research focuses on the discovery, exploitation, and remediation of software vulnerabilities, analysis of malicious code, and evaluation of security software. Chris has published a number of advisories and technical white papers based on his research. He has also contributed to several books on information security.

Chris holds a bachelor's degree in Computer Science with a Mathematics Minor from Colby College, where he completed research involving automated malicious code detection. Chris has also worked as an analyst at the National Cyber-Forensics & Training Alliance (NCFTA), where he conducted technical research to support law enforcement.

Chris tech-edited Chapters 8 and 9.

Carsten Willems is an independent software developer with 10 years' experience. He has a special interest in the development of security tools related to malware research. He is the creator of the CWSandbox, an automated malware analysis tool. The tool, which he developed as a part of his thesis for his master's degree in computer security at RWTH Aachen, is now distributed by Sunbelt Software in Clearwater, FL. He is currently working on his PhD thesis, titled "Automatic Malware Classification," at the University of Mannheim. In November 2006 he was awarded third place at the Competence Center for Applied Security Technology (CAST) for his work titled "Automatic Behaviour Analysis of Malware." In addition, Carsten has created several office and e-business products. Most recently, he has developed SAGE GS-SHOP, a client-server online shopping system that has been installed over 10,000 times.

Carsten wrote Chapter 10.