About the Authors

Ofir Arkin is the founder of the Sys-Security Group, a nonbiased computer security research and consultancy body. He has worked as a consultant for several major European finance institutes were he played the role of Chief Security Architect and Senior Security Architect. He also acted as Chief Security Architect for a 4th generation telecom company, where he designed the overall security architecture for the company. Currently Ofir is the CISO of a leading telecom company in Israel. Ofir has published several papers as well as articles and advisories, including "Etherleak: Ethernet frame padding information leakage," "Security Risk Factors with IP Telephony based Networks," the "ICMP Usage in Scanning" research paper, Xprobe2 (tool and paper), "The Cisco IP Phones Compromise," and "Trace-Back." Ofir has lectured in a number of information security conferences (such as the Blackhat briefings) and is a co-author of the first edition of *Know Your Enemy* (Addison-Wesley, 2003).

Edward Balas is a security researcher within the Advanced Network Management Laboratory at Indiana University. Edward's professional interest focuses on network infrastructure protection. As a member of the Honeynet Project, Edward has lead the development of Sebek. Prior to joining Indiana University, Edward spent over 5 years in the network industry as a engineer at a tier-1 ISP and as a developer of network management systems.

Brian Carrier is the author of several digital forensic analysis tools, including The Sleuth Kit and the Autopsy Forensic Browser. His research at CERIAS (Purdue University) involves digital forensic analysis tools and procedures. Previously, he was a Research Scientist at @stake, where he led the @stake

Response Team and Digital Forensic Labs. Brian has taught forensics and incident response at SANS, FIRST, and the @stake Academy and has given talks at many conferences on his tools and computer forensics. Brian has also presented at the FBI Academy and other U.S. military and intelligence agencies with the Honeynet Project.

Roshen Chandran is a co-founder of Paladion Networks and focuses on building a great place to work. Roshen enjoys designing solutions for clients and testing the security of their applications. He graduated from the College of Engineering, Trivandrum and completed an MBA from XLRI, Jamshedpur, India. Roshen worked closely with the Paladion team of Shaheem Motlekar and Giridhar T M to develop the chapter on Network Forensics.

Anton Chuvakin, Ph.D., GCIA, is a Senior Security Analyst with netForensics, a security information management software company that provides real-time network security monitoring solutions. His areas of infosec expertise include intrusion detection, UNIX security, forensics, and honeypots. He has written numerous articles and book reviews on computer and network security published by SecurityFocus, "Linux Journal," ";login," ISSA "Password," "SC Magazine" online and LinuxSecurity.com, ComputerWorld.com and has presented to various security organizations. Anton has also contributed to "SANS Top 20 Vulnerabilities" (2002, 2003), SANS "Step-by-step" guides and is an active member of the GCIA Certification Advisory Board. In his spare time he maintains his security portal. He is the author of the book *Security Warrior* (O'Reilly, 2004).

Michael Clark became involved with the Honeynet Project several years ago. The areas he has contributed to most have been virtual honeynets, data analysis, and Sebek. Professionally, Michael has worked for the University of Pennsylvania, Lockheed Martin, and Mantech Aegis Research Corporation. He has also spoken at the FBI Academy, West Point Military Academy, National Security Agency, JTF-CNO, and several conferences. In his free time, Michael enjoys games, movies, astronomy, basketball and spending time with his wife, Lisa.

Eric Cole is a highly sought after network security consultant and speaker. He has consulted for international banks and Fortune 500 companies, and has provided advice to venture capitalist firms on what startups should be funded. He

has in-depth knowledge of network security and has come up with creative ways to secure his clients' assets and is author of several books including *Hackers Beware* and *Hiding in Plain Sight*. He holds several patents and has written numerous magazine and journal articles. He worked for the CIA for over 7 years and has created several successful network security practices. Eric is a member of the CVE Editorial board, an invited position. He presents at a variety of conferences including SANS where he helped create several of the courses and has been interviewed by CBS news, 60 Minutes and CNN. He is currently in charge of research and the chief scientist for The Sytex Group.

Yannis Corovesis is head of the Internet Systematics Lab at the National Center for Science Research in Athens. He holds a Ph.D. in Computer Science and is an Internet pioneer in Greece. In the early 90s he contributed to the book *Internet: Getting Started* under SRI's coordination. He considers knowledge communication about Internet systems with Free/Open software a killer application.

Jeff Dell is founder of Activeworx, Inc., a security software and consulting company. Mr. Dell specializes in enterprise security design, Security Audit, and intrusion detection systems. Mr. Dell has over ten years of experience in networking and security, including positions as Chief Information Security Officer at Seisint, Inc., a supercomputer/data mining company and Director of Information Security at TelePlace, Inc. In his free time Mr. Dell develops free windows security software, including, among others, IDS Policy Manager and Honeynet Security Console. Mr. Dell also sits on the SANS GCIA advisory board, a SANS Local Mentor Instructor. Jeff has a Bachelors degree from Arizona State University and has achieved the GCIA and CISSP certifications.

J. Raul Garcia Zapata is an IP network specialist at AT&T Mexico. Nowadays most of his work is related to network security. Years ago, in the early 90s, he worked on his first coax ethernet network and that's where it all started for him. It was during this time that he first got to use Linux, long before its GUI was what it is now. Now he not only manages security for large IP backbones but also oversees new services and manages security devices that span Mexico.

Max Kilger is a social psychologist whose first programming encounter with a PDP8-I in 1968 hooked him on computational machines for life. It was during

his graduate school years at Stanford that he first came to notice and become fascinated with the ways in which technology changes how people perceive machines, as well as how it alters the way in which people think and perceive their own social world. It was here that his interest in the social psychology of the hacking community was born. After receiving his Ph.D. from Stanford he taught at the City University of New York where he established one of the first undergraduate courses on the effects of digital technology on society. He is a member of the National Academy of Engineering's Combatting Terrorism Committee. Max currently works for a research firm leading the development of statistical strategies for building behavioral systems that span databases of disparate individuals, allowing the prediction of behavior in sparse data environments. As a member of the Honey Project he continues to research the social structure of the whitehat/blackhat communities and is a frequent speaker to computer security organizations and federal agencies.

Charalambos Koutsouris is a network engineer at the Internet Systematics Lab at the National Center for Science Research in Athens, Greece. His main areas of work are network design and secure network perimeters. He is involved with network forensics and is studying for an M.Sc. in Data Communications.

Richard LaBella has been actively involved in computer and network security since 1996 after discovering L0pht Heavy Industries. The L0pht showed Richard a new area of computing that changed his life forever—Digital Security. In 1998 Richard built his first firewall for a small telecommunications company using spare parts he found in a closet of abandoned hardware. In 1999 Richard was offered a lead position with a dot com startup in Miami to design and build an Enterprise, E-commerce procurement system whose purpose was to provide centralized procurement for the boating industry. In 2001, Richard discovered the Honeynet Project, founded his own nonprofit honeynet organization, the Florida Honeynet Project, and cofounded the Honeynet Research Alliance with Lance Spitzner and Mike Clark in January 2002. Richard has been actively involved in learning the motives, tools, and tactics of the enemy ever since. Richard has spoken publicly about honeynet research for West Point Military Academy, The Pentagon, The FBI, The NSA, and other organizations such as Infragard and ISSA. Today, Richard continues to plan, design, deploy, and manage many aspects of digital security for business.

Rob Lee is a member of the Computer Forensics & Intrusion Analysis Division of ManTechs National Security Solutions Group, which provides advanced computer forensics and intrusion operations support to the national security and intelligence communities. He enjoys working on a variety of technical projects including incident response, forensics, intrusion detection, vulnerability analysis, and specialized R&D. He has presented regularly for SANS, where he has authored several courses. Rob is a graduate of the U.S. Air Force Academy. He served in the U.S. Air Force performing intrusion detection while at the 609th Information Warfare Squadron. As a member of the Air Force Office of Special Investigations he performed network wiretaps and conducted computer crime intrusion investigations. Rob conducted the first wireless honeynet in the DC area in 2002.

Costas Magkos is a network manager at the Internet Systematics Lab at the National Center for Science Research in Athens, Greece. He holds an M.Sc. in Data Communications. His expertise is in the area of network operations and network development. He is interested in modern backbone technologies and Open Source-based IT security.

Patrick McCarty is currently pursuing a degree in Computer Science from Azusa Pacific University in Azusa, CA, and will graduate in May of 2004. He is currently serving as president of APU's chapter of ACM (Association for Computing Machinery). When not working or studying, he spends time furthering honeynet research.

Dion Mendel names himself a Computer Programmer, shunning the pretentious titles found in the computing industry. Before winning the Honeynet Reverse Challenge in 2002, his experience with reverse engineering was predominantly concerned with reversing file formats. Since that time he has shifted his focus to reversing executables. The lack of available information on reverse engineering has prompted him to begin to document those techniques and skills. His desire is for reverse engineering to become a widely available skill, and to cease being the misunderstood black art it is currently seen to be.

Yannis Papapanos is a vocational student at the Technical Institute of Athens in the Internet Systematics Lab at the National Center for Science Research in Athens, Greece. He is involved with the deployment of the Lab's GenII Honeynets. He is experimenting with a SNORT module for ICMP spoof detection.

Richard P. Salgado serves as Senior Counsel in the Computer Crime and Intellectual Property Section of the United States Department of Justice. Mr. Salgado specializes in investigating and prosecuting computer network cases, such as computer hacking, illegal computer wiretaps, denial of service attacks, malicious code, and other technology-driven privacy crimes. Mr. Salgado also regularly trains investigators and prosecutors on the legal and policy implications of searching and seizing computers and electronic evidence, emerging surveillance technologies, and related criminal conduct. He participates in policy development relating to emerging technologies such as the growth of wireless networks, voice-over Internet Protocol, surveillance tools, and forensic techniques. Mr. Salgado is an adjunct law professor at Georgetown University Law Center, where he teaches a Computer Crime seminar, and is a faculty member of the SANS Institute and the National Judicial College. Mr. Salgado graduated magna cum laude from the University of New Mexico and in 1989 received his J.D. from Yale Law School.

Lance Spitzner is a geek intrigued by the strategies and tactics of information security. This interest first began in the military, where he served for seven years, four as an Armor officer in the Army's Rapid Deployment Force. Following the military he earned his M.B.A. and became involved in the world of information security. His passion is researching honeypot technologies and using them to learn more about cyberthreats. He is founder of the Honeynet Project, moderator of the honeypot mail-list, author of *Honeypots: Tracking Hackers* (Addison-Wesley, 2003), co-author of the first edition of *Know Your Enemy* and author of several whitepapers. He has also spoken at various conferences and organizations, including SANS, Blackhat, FIRST, the Pentagon, the FBI Academy, the President's Advisory Board, the Army War College, West Point, and Navy War College.

Jeff Stutzman is currently employed by Cisco Systems, Computer Security Programs Office. He is a former US Navy Intelligence Officer from the computer warfare field of Information Warfare, and an enlisted US Coast Guard systems administrator. Mr. Stutzman spent two years as a visiting scientist with Carnegie Mellon Universities Software Engineering Institute. Mr. Stutzman is the founder of both ZNQ3 and Beadwindow! Published works include the first edition of *Know Your Enemy,* and several technical papers in the field of information security.