Cyber Hard Problems

Committee

John L. Manferdelli

Chair

John Manferdelli, chair of the forum on cyber resilience is an independent consultant. Before that, he was, most recently, Confidential Computing, Incubation Project Leader in the Office of the CTO at VMware. Previously, he was Professor of the Practice and executive director of the Cybersecurity and Privacy Institute at Northeastern University. Immediately prior, Manferdelli was Engineering Director for Production Security Development at Google. Prior to Google, he was a senior principal engineer at Intel Corporation and co-PI (with David Wagner) for the Intel Science and Technology Center for Secure Computing at the University of California at Berkeley. He was also a member of the Information Science and Technology advisory group at DARPA and is a member of the Defense Science Board. Prior to Intel, J Manferdelli was a distinguished engineer at Microsoft and was an affiliate faculty member in computer science at the University of Washington. He was responsible for computer security, cryptography, and systems research, as well as research in quantum computing. At Microsoft, John also worked as a senior researcher, software architect, product unit manager, general manager at Microsoft and was responsible the development of the next-generation secure computing base technologies and the rights management capabilities currently integrated into Windows, for which he was the original architect. He joined Microsoft in February 1995 when it acquired his company, Natural Language Inc., based in Berkeley, California. At Natural Language, Manferdelli was the founder and, at various times, vice president of research and development and CEO. Other positions he has held include staff engineer at TRW Inc., computer scientist and mathematician at Lawrence Livermore National Laboratory, and principal investigator at Bell Labs. He was also an adjunct associate professor at Stevens Institute of Technology. Manferdelli’s professional interests include cryptography and cryptographic mathematics, combinatorial mathematics, operating systems, and computer security. He is also a licensed Radio Amateur (AI6IT). Manferdelli has a bachelor’s degree in physics from Cooper Union for the Advancement of Science and Art and a PhD in mathematics from the University of California, Berkeley.

Hyrum Anderson

Member

Hyrum Anderson is CTO at Robust Intelligence. Much of his career has been focused on defense and security, having directed research projects at MIT Lincoln Laboratory, Sandia National Laboratories, Mandiant, as Chief Scientist at Endgame (acquired by Elastic), and Principal Architect of Trustworthy Machine Learning at Microsoft. While at Microsoft, he organized Microsoft's AI Red Team and oversaw the first exercises on production AI systems as chair of the AI Red Team governing board. Hyrum co-founded the Conference on Applied Machine Learning in Information Security (CAMLIS) and co-organizes the ML Security Evasion Competition and the ML Model Attribution Challenge. He has spoken at numerous academic and industry conferences at the intersection of security and machine learning, including RSA, BlackHat and DEFCON. He has authored over 60 peer-reviewed academic publications, and co-authored the book "Not With a Bug, But With a Sticker: Attacks on Machine Learning Systems and What To Do About Them". He received his PhD in Electrical Engineering from the University of Washington, with an emphasis on signal processing and machine learning, and BS and MS degrees in Electrical Engineering from Brigham Young University.

Josiah Dykstra

Member

Josiah Dykstra is the Director of Strategic Initiatives at Trail of Bits. He previously served for 19 years as a senior technical leader at the National Security Agency (NSA). Dr. Dykstra is an experienced cyber practitioner and researcher whose focus has included the psychology and economics of cybersecurity. He received the CyberCorps® Scholarship for Service (SFS) fellowship and is one of six people in the SFS Hall of Fame. In 2017, he received the Presidential Early Career Award for Scientists and Engineers (PECASE) from then President Barack Obama. Dr. Dykstra is a Fellow of the American Academy of Forensic Sciences (AAFS) and a Distinguished Member of the Association for Computing Machinery (ACM). He is the author of numerous research papers, the book Essential Cybersecurity Science (O'Reilly Media, 2016), and co-author of Cybersecurity Myths and Misconceptions (Pearson, 2023). Dr. Dykstra holds a Ph.D. in computer science from the University of Maryland, Baltimore County.

Paul England

Member

Paul England (NAE) is a distinguished engineer and manager of a team of researchers and engineers in Microsoft Research. Paul led or contributed to many of the computer industry’s hardware-based security innovations over the last 20 years. Most notable is the field of Trusted and Confidential Computing: a combination of novel cryptographic operations together with hardware/software environments for secure computation. Trusted Computing primitives are now a feature of most mobile, client, server, and cloud computer systems, and the field remains an area of active research. Paul also contributed to the design of the first Trusted Platform Module and led the team that developed the current version. Paul became interested in cyber-resilient systems through his work with NIST in developing NIST SP 800-193 – Platform Firmware Resiliency Guidelines. Based on this, he subsequently worked with hardware partners and standards groups to develop architectures and hardware/software building blocks to enable secure and high-assurance recovery of devices that have been compromised by malware or misconfiguration. Dr. England received his Ph.D. in condensed matter physics from Imperial College, London.

Maritza Johnson

Member

Maritza Johnson is an expert on human-centered security and privacy with industry, teaching, and research experience, she is currently a director at Good Research where she works with companies to build technological solutions that people can use safely. In prior roles, Maritza was the Founding Director of the Center for Digital Civil Society at the University of San Diego, a User Experience Researcher at Google Research, and a Technical Privacy Manager on Facebook's Public Policy team. She’s a member of the National Academy of Science Forum on Cyber Resilience and an advisor to Confidencial. In 2011, her paper "The Failure of Online Social Network Privacy Settings" won the Future of Privacy Forum's Privacy Papers for Policy Makers Award. Maritza received M.S. and Ph.D. degrees in computer science from Columbia University in 2008 and 2012, and a B.A. degree from the University of San Diego in 2005.

Angelos D. Keromytis

Member

Angelos D. Keromytis is John H. Weitnauer Endowed Chair Professor and Georgia Research Alliance (GRA) Eminent Scholar at the Georgia Institute of Technology. His field of research is systems and network security and applied cryptography. He joined Georgia Tech from DARPA, where he served as Program Manager in the Information Innovation Office (I2O) from 2014 to 2018. During that time, he initiated five major research initiatives in cybersecurity and managed a portfolio of nine programs, and supervised technology transitions and partnerships with numerous elements of the Department of Defense, the Intelligence Community, Law Enforcement, and other parts of the U.S. government. For his work, he received the DAPRA Superior Public Service Medal. Before DARPA, he served as Program Director with the Computer and Network Systems Division in the Directorate for Computer and Information Science & Engineering (CISE) at the National Science Foundation (NSF), where he co-managed the Secure and Trustworthy Cyberspace (SaTC) program and helped initiate a number of cross-disciplinary and public-private programs. Prior to his public service tour, Dr. Keromytis was a faculty member of the Department of Computer Science at Columbia University, where he founded the Network Security Lab. Dr. Keromytis is an elected Fellow of the ACM and the IEEE. He has 63 issued U.S. patents and over 250 refereed publications. His work has been cited over 28,000 times, with an h-index of 83 and i10-index of 260. He has founded four new technology ventures and is currently serving as President for two of them. He is a certified PADI Master Instructor, with over 700 dives. He received his Ph.D. (2001) and M.Sc. (1997) in Computer Science from the University of Pennsylvania, and his B.Sc. in Computer Science from the University of Crete, Greece.

Wendy Nather

Member

Wendy Nather is the Senior Research Initiatives Director at 1Password. She was previously Director of Advisory CISOs at Duo Security, and Research Director at the Retail ISAC, where she was responsible for advancing the state of resources and knowledge to help organizations defend their infrastructure from attackers. Wendy was also Research Director of the Information Security Practice at independent analyst firm 451 Research, covering the security industry in areas such as application security, threat intelligence, security services, and other emerging technologies. Wendy has served as a CISO in both the private and public sectors. She led IT security for the EMEA region of the investment banking division of Swiss Bank Corporation (now UBS), as well as for the Texas Education Agency. Wendy is co-author of The Cloud Security Rules and Splunk's Bluenomicon. She was inducted into the Infosecurity Europe Hall of Fame in 2021. She serves on the board of directors for Sightline Security, an organization that helps provide free security assessment services to nonprofit groups. Wendy is a Senior Fellow at the Atlantic Council's Cyber Statecraft Initiative, and a steering committee member for the IST Ransomware Task Force.

Stefan Savage

Member

Stefan Savage is the Irwin and Joan Jacobs professor of Information and Computer Science at the University of California, San Diego. He currently serves as the co-director for UCSD's Center for Network Systems (CNS) and as a founding member of the school’s Center for Healthcare Cybersecurity. Savage is known for his work on network security and reliability, on cybercrime economics and defense, and on the empirical measurement of cybersecurity and cyberinfrastructure. He is a member of the National Academy of Engineering and the American Academy of Arts and Sciences, a MacArthur Fellow, an ACM Fellow, and is the recipient of ACM's Prize in Computing and AAAS' Golden Goose award. He received his Ph.D. in Computer Science and Engineering from the University of Washington and a B.S. in Applied History from Carnegie Mellon University.

William L. Scherlis

Member

William L. Scherlis is a Professor of Computer Science at Carnegie Mellon University and Special Advisor to the Software Engineering Institute, a DoD FFRDC at CMU. He recently served as director of DARPA’s Information Innovation Office (I2O) leading program managers in the development of programs in cybersecurity, artificial intelligence, secure software, and information operations. At Carnegie Mellon (CMU) he served for more than a decade as head of the Software and Societal Systems Department, which hosts research and educational programs related to software development, security and privacy, IoT and mobility, AI engineering, social network analysis, and related topics. He founded the CMU PhD program in Software Engineering and led it for its first decade. His research relates to software assurance, cybersecurity, software analysis, and assured safe concurrency. He has led several large research projects including the CMU National Security Agency Science of Security Lablet and the CMU/NASA High Dependability Computing Project. He served as program chair for technical conferences including ACM Foundations of Software Engineering (FSE) and ACM Partial Evaluation and Program Manipulation (PEPM). Scherlis has led multiple national studies including the National Academies study that in 2010 produced the report Critical Code: Software Producibility for Defense. He has testified before Congress on the federal AI workforce, on federal software sustainment, on computing technology and innovation, and on roles for a Federal CIO. He is a Life Fellow of the IEEE and a Lifetime National Associate of the National Academy of Sciences. Dr. Scherlis received an AB magna cum laude from Harvard University in applied mathematics and a PhD in computer science from Stanford University, with an intervening year in the Department of Artificial Intelligence at the University of Edinburgh as a John Knox Fellow.

Mark Seiden

Member

Mark Seiden currently serves as the Security Advisor to the Internet Archive and holds the position of associate professor in Computer Science at Columbia University. In addition, he is engaged in a DARPA-funded research project with UC Santa Cruz and has offered his expertise in around 50 criminal and civil cases. With a programming career that spans since the '60s, Mark has collaborated with diverse companies and research institutions, making significant contributions to software engineering, network technologies, operating systems, and physical security. In recent years, Mark Seiden has dedicated 15 years to the ICANN Security and Stability Advisory Committee and actively participated in multiple National Academy of Sciences studies addressing technological risk. His noteworthy affiliations include roles at IBM Research, Lucasfilm, Yahoo, Xerox PARC, Bell Labs, Bellcore, and IRCAM. Mr. Seiden earned his SM degree in Computer Science and Electrical Engineering from Columbia University in 1981.

Window Snyder

Member

Window Snyder is a security industry pioneer and CEO and Founder of Thistle Technologies. Ms. Snyder is the former Chief Security Officer at Square and Fastly. She previously spent five years at Apple responsible for security and privacy strategy and features for OS X and iOS. Other roles include Chief Software Security Officer at Intel, Chief Security Something-or-Other at Mozilla and a founder at Matasano, a security services and product company based in New York. Ms. Snyder is co-author of Threat Modeling, a manual for security architecture analysis in software.

Mary Ellen Zurko

Member

Mary Ellen Zurko is a technical staff member at the Massachusetts Institute of Technology (MIT) Lincoln Laboratory. She has worked in product development, early product prototyping, and research and has more than 20 patents. She defined the field of user-centered security in 1996, and has worked in cybersecurity for over 35 years. She was the security architect of one of IBM’s earliest clouds. She was a founding member of the National Academies’ Forum on Cyber Resilience and serves as a Distinguished Expert for NSA’s Best Scientific Cybersecurity Research Paper competition. Her research interests include unusable security for attackers, Zero Trust architectures for government systems, security development and code security, authorization policies, high-assurance virtual machine monitors, the web, and PKI. Zurko received a S.B. and S.M. in computer science from MIT. She has been the only “Mary Ellen Zurko” on the web for over 25 years.