Future of Encryption

Committee

Steven B. Lipner

Chair

Mr. Steven B. Lipner (NAE) is executive director of SAFECode, a non-profit organization dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods. He retired in 2015 as partner director of software security in Trustworthy Computing at Microsoft Corporation. His expertise is in software security, software vulnerabilities, Internet security, and organization change for security. He is the founder and long-time leader of the Security Development Lifecycle (SDL) team that has delivered processes, tools and associated guidance, and oversight that have significantly improved the security of Microsoft's software. Mr. Lipner has over 40 years of experience as a researcher, development manager, and general manager in IT security. He served as executive vice president and general manager for Network Security Products at Trusted Information Systems and has been responsible for the development of mathematical models of security and of a number of secure operating systems. Mr. Lipner was one of the initial 12 members of the U.S. Computer Systems Security and Privacy Advisory Board (now the Information Security and Privacy Advisory Board) and served two terms and a total of ten years on the board. He is the author of numerous professional papers and has spoken on security topics at many professional conferences. He is named as inventor on 12 U.S. patents in the fields of computer and network security and has served on numerous scientific boards and advisory committees, including as a current member of the NRC Committee on Future Research Goals and Directions for Foundational Science in Cybersecurity and the NRC Committee on Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs. Mr. Lipner was elected in 2015 to the National Cybersecurity Hall of Fame and in 2017 to the National Academy of Engineering.

Mark Lowenthal

Vice Chair

Dr. Mark Lowenthal is president emeritus of the Intelligence & Security Academy, LLC, a national security education, training and consulting company where he was formerly president and chief executive officer. Dr. Lowenthal is an internationally recognized expert on intelligence. He is also on the faculty at the Krieger School of Arts and Sciences at Johns Hopkins University in Washington, D.C. and Sciences Po in Paris. From 2002-2005, Dr. Lowenthal served as the assistant director of Central Intelligence for Analysis and Production and as the vice chairman for evaluation on the National Intelligence Council. Prior to these duties, he served as counselor to the director of Central Intelligence. Dr. Lowenthal has written extensively on intelligence and national security issues, including six books and over 100 articles or studies. His most recent book, Intelligence: From Secrets to Policy (Sage/CQ Press, 8th ed., 2019) has become the standard college and graduate school textbook on the subject. Dr. Lowenthal received his B.A. from Brooklyn College and his Ph.D. in history from Harvard University and was awarded the National Intelligence Distinguished Service Medal, the intelligence community's highest award. Dr. Lowenthal is a former staff director of the House Permanent Select Committee on Intelligence.

Hans R. Davies

Member

Mr. Hans Robert Davies is a futurist at Toffler Associates. Hans specializes in strategic planning, risk management, resource management, and innovation policy. He helps organizations strengthen their ability to manage enterprise risk. Prior to joining Toffler Associates, Hans worked at SAIC, supporting arms control and complex operations initiatives for the Department of Defense. He has served as a Congressional staff member, worked with the Department of State, and was a Robert Bosch Foundation Fellow in Germany. Hans earned a B.A. with honors in History from Williams College and an M.A. in International Relations and International Economics from Johns Hopkins University.

Chip Elliott

Member

Mr. Chip Elliott recently retired from serving as the chief technology officer at BBN Technologies. He is an American engineer, best known for his work in creating advanced computer networks. He graduated from Dartmouth College, where he maintained and helped create computer language systems, including Algol 60, APL, Dynamo, and PL/I, for the Dartmouth Time Sharing System. Subsequently, he was a founder of True BASIC, Inc. At BBN Technologies in the 1990s, he created the videoconferencing system for the Defense Simulation Internet, led the networking design and implementation of the Iris Digital Communications System, and served as network architect for the Near-term digital radio (NTDR) system. He also participated in the design of Connexion by Boeing, Celestri, Discoverer II, and SBIRS-Low. In early 2000, Elliott led the design and build-out of the DARPA Quantum Network, which was the world's first quantum cryptography network, operating 10 optical nodes across the Boston region to provide highly secure key distribution non-stop through both telecom fibers and the atmosphere. He then served as the founding project director for GENI, the Global Environment for Network Innovations, a national suite of experimental infrastructure created across more that 60 university campuses by the National Science Foundation for at-scale research in future internet architectures, services, and security. Elliott has served on panels in the U.S. including for the Defense Science Board and Army, Navy, SOCOM, and DTO boards, and has held visiting and adjunct faculty positions at Dartmouth College, Tunghai University in Taiwan, and the Indian Institute of Technology, Kanpur. He holds over 90 issued patents, and has been named a fellow of the American Association for the Advancement of Science, ACM Fellow, and Fellow of the Institute of Electrical and Electronics Engineers. For his leadership in quantum cryptography he was given Frost & Sullivan's Award for Excellence in Technology (2005) and named a World Technology Award Finalist (2004) and Fellow.

Glenn S. Gerstell

Member

Mr. Glenn S. Gerstell is senior adviser at the Center for Strategic and International Studies. He served as the general counsel of the National Security Agency (NSA) and Central Security Service (CSS) from 2015 to 2020. He has written and spoken widely about the intersections of technology and national security and privacy. Prior to joining the NSA, Mr. Gerstell practiced law for almost 40 years at the international law firm of Milbank, LLP, where he focused on the global telecommunications industry and served as the managing partner of the firm's Washington, D.C., Singapore, and Hong Kong offices. Mr. Gerstell served on the President's National Infrastructure Advisory Council, which reports to the president and the secretary of homeland security on security threats to the nation's infrastructure, as well as on the District of Columbia Homeland Security Commission. A graduate of New York University and Columbia University School of Law, Mr. Gerstell is an elected member of the American Academy of Diplomacy and a member of the Council on Foreign Relations. Earlier in his career, he was an adjunct law professor at the Georgetown University Law Center and New York Law School. He is a recipient of the National Intelligence Distinguished Service Medal, the Secretary of Defense Medal for Exceptional Civilian Service and the NSA Distinguished Civilian Service Medal.

Nadia Heninger

Member

Dr. Nadia Heninger is an associate professor in computer science and engineering at the University of California-San Diego. Her research focuses on applied cryptography and security, particularly cryptanalysis of public-key cryptography in practice. She is the recipient of a 2017 NSF CAREER award, and her research has won best paper awards at CCS 2016, CCS 2015, Usenix Security 2012, and a best student paper award at Usenix Security 2008. Previously, she was an assistant professor at the University of Pennsylvania. She received her Ph.D. in computer science in 2011 from Princeton and spent time as a postdoc at University of California-San Diego and Microsoft Research New England.

Seny Kamara

Member

Dr. Seny Kamara is an associate professor of computer science at Brown University and chief scientist at Aroki Systems. Before joining Brown, he was a researcher at Microsoft Research (Redmond Lab). His research is in cryptography and is driven by real-world problems from privacy, security, and surveillance. He has worked extensively on the design and cryptanalysis of encrypted search algorithms, which are efficient algorithms to search on end-to-end encrypted data. He maintains interests in various aspects of theory and systems, including applied and theoretical cryptography, data structures and algorithms, databases, networking, game theory and technology policy. He also directs the Encrypted Systems Lab and is affiliated with the CAPS group, the Data Science Initiative, and the Center for Human Rights and Humanitarian Studies.

Paul C. Kocher

Member

Mr. Paul Carl Kocher (NAE) is an American cryptographer and cryptography entrepreneur who founded Cryptography Research, Inc. (CRI) and served as its president and chief scientist. He received a bachelor's degree in biology from Stanford University in 1995, where he worked part-time with Martin Hellman. As demand for Kocher's knowledge in cryptography escalated, he gave up on his original plan to become a veterinarian and founded CRI instead. Kocher pioneered the field of side-channel attacks, including the development of timing attacks that can break implementations of RSA, DSA and fixed-exponent Diffie–Hellman that operate in non-constant time, as well as the co-development of power analysis and differential power analysis. His side-channel attack countermeasure designs are widely deployed in secure integrated circuits and other cryptographic devices. He has also worked on microprocessor security, and co-discovered and named the Spectre vulnerability, which leverages speculative execution and other microprocessor performance optimizations to extract confidential information. He also helped architect security-related integrated circuits, including Deep Crack, a DES brute-force key search machine.

Brian LaMacchia

Member

Dr. Brian LaMacchia is a Distinguished Engineer at Microsoft Corporation and heads the Security and Cryptography team within Microsoft Research (MSR). His team's main project at present is the development of quantum-resistant public-key cryptographic algorithms and protocols. Brian is also a founding member of the Microsoft Cryptography Review Board and consults on security and cryptography architectures, protocols and implementations across the company. Before moving into MSR in 2009, Brian was the architect for cryptography in Windows Security, Development Lead for .NET Framework Security and program manager for core cryptography in Windows 2000. Prior to joining Microsoft, Brian was a member of the Public Policy Research Group at AT&T Labs—Research. In addition to his responsibilities at Microsoft, Brian is an adjunct associate professor in the School of Informatics and Computing at Indiana University-Bloomington and an affiliate faculty member of the Department of Computer Science and Engineering at the University of Washington. Brian also currently serves as treasurer of the International Association for Cryptologic Research (IACR) and as a vice president of the Board of Directors of Seattle Opera. Brian received S.B., S.M., and Ph.D. degrees in electrical engineering and computer science from the Massachusetts Institute of Technology (MIT) in 1990, 1991, and 1996, respectively.

Butler W. Lampson

Member

Dr. Butler W. Lampson (NAS, NAE) is a technical fellow at Microsoft Corporation and an adjunct professor at MIT. He has worked on computer architecture, local area networks, raster printers, page description languages, operating systems, remote procedure call, programming languages and their semantics, programming in the large, fault-tolerant computing, transaction processing, computer security, WYSIWYG editors, and tablet computers. He was one of the designers of the SDS 940 time-sharing system, the Alto personal distributed computing system, the Xerox 9700 laser printer, two-phase commit protocols, the Autonet LAN, the SPKI system for network security, the Microsoft Tablet PC software, the Microsoft Palladium high-assurance stack, and several programming languages. He received the ACM Software Systems Award in 1984 for his work on the Alto, the IEEE Computer Pioneer award in 1996 and von Neumann Medal in 2001, the Turing Award in 1992, and the NAE's Draper Prize in 2004. He is a member of the National Academy of Sciences and the National Academy of Engineering and a fellow of the Association for Computing Machinery and the American Academy of Arts and Sciences.

Rafail Ostrovsky

Member

Dr. Rafail Ostrovsky is a Distinguished Professor of Computer Science and Distinguished Professor of Mathematics at UCLA. Prof. Ostrovsky joined UCLA in 2003 as a full tenured professor, coming from Bell Communications Research where he was a Senior Research Scientist. Prior to beginning his career at Bellcore, he was an NSF Mathematical Sciences Postdoctoral Research Fellow at UC Berkeley. Dr. Ostrovsky received his Ph.D. in computer science from MIT in 1992, (advisor: Silvio Micali, thesis: Software Protection and Simulation on Oblivious RAM), supported by IBM Graduate Fellowship. Prof. Ostrovsky is a Fellow of IEEE; Fellow of IACR; and a foreign member of Academia Europaea. He has 14 U.S. patents issued and over 300 papers published in refereed journals and conferences. Dr. Ostrovsky has served as a Chair of the IEEE Technical Committee on Mathematical Foundations of Computing from 2015-2018 and has served on over 40 international conference Program Committees including serving as PC chair of FOCS 2011. He is a member of the Editorial Board of Journal of ACM; Editorial Board of Algorithmica; and the Editorial Board of Journal of Cryptology and is the recipient of multiple awards and honors including the 2017 IEEE Computer Society Technical Achievement Award and the 2018 RSA Conference Excellence in the Field of Mathematics lifetime achievement Award. At UCLA, Prof. Ostrovsky heads the Center of Information and Computation Security (CICS) a multi-disciplinary Research Center (http://www.cs.ucla.edu/security/) at Henry Samueli School of Engineering and Applied Science.

Elizabeth Rindskopf Parker

Member

Ms. Elizabeth Rindskopf Parker retired as the executive director of the State Bar of California. She previously served as the dean of the McGeorge School of Law at the University of the Pacific from 2002 to 2012. She was general counsel with the University of Wisconsin system from 1999 to 2002. Before that, she was general counsel of the Central Intelligence Agency from 1990 to 1995. She was also the principal deputy legal advisor to the Department of State and general counsel for the National Security Agency. She received her J.D. from the University of Michigan. She is a lifetime counselor and former chair of the ABA Standing Committee on Law and National Security and holds membership in the American Bar Foundation and the Council on Foreign Relations. She has served on a number of committees at the National Academies of Sciences, Engineering, and Medicine. Parker is also a two-term presidential appointee to the Public Interest Declassification Board.

Peter Swire

Member

Peter Swire is the Elizabeth and Tommy Holder Chair of Law and Ethics at the Georgia Tech Scheller College of Business, where he teaches cybersecurity and privacy. He is senior counsel with Alston & Bird LLP, Research Director for the Cross-Border Data Forum, and a member of the National Academies of Science and Engineering Forum on Cyber Resilience. In 2018, he was named an Andrew Carnegie Fellow for his project on cross-border data flows. In 2015 the International Association of Privacy Professionals awarded him its Privacy Leadership Award. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. In 2009-10, he served as Special Assistant to President Obama for Economic Policy. Under President Clinton, Swire was the Chief Counselor for Privacy, the first person to have U.S. government-wide responsibility for privacy policy. In that role, his activities included being White House coordinator for the HIPAA medical privacy rule, and chairing the White House working group on encryption. He graduated from Princeton University and the Yale Law School.

Peter J. Weinberger

Member

Dr. Peter J. Weinberger is a software engineer at Google. He is a computer scientist best known for his early work at Bell Labs. He was an undergraduate at Swarthmore College, graduating in 1964. He received his Ph.D. in mathematics in 1969 from the University of California, Berkeley in Number Theory. After holding a position in the department of mathematics at the University of Michigan, Ann Arbor, where he continued his work in number theory, he moved to AT&T Bell Labs, where he contributed to the design of the AWK programming language (he is the "W" in AWK), and worked on database systems, and a Fortran compiler. Prior to joining Google, Dr. Weinberger was at Renaissance Technologies, a hedge fund. He is a fellow of the AAAS, and is on various committees giving technical advice to the U.S. government.