DAVID M. BALENSON

SRI International
1100 Wilson Blvd, Suite 2800, Arlington, VA 22209
(703) 247-8551, david.balenson@sri.com

SUMMARY OF EXPERIENCE

Mr. Balenson has 35 years of experience leading organizations and efforts to research, develop, test, evaluate, and transition innovative solutions to challenging cybersecurity needs and requirements. His current research interests include cybersecurity for critical infrastructure and cyber-physical systems, experimentation and test, technology transition, and multi-disciplinary research. He has broad-based experience and background in critical infrastructure security and resilience, computer and network security, applied cryptography, and R&D program and project management.

He provides technical and programmatic expertise for the U.S. Department of Homeland Security Science and Technology Directorate (DHS S&T). Currently supported projects include the Commercialization Accelerator Program (CAP). Past projects include the Automotive Cybersecurity Industry Consortium (ACIC), Cybersecurity for Oil and Gas Systems (COGS), Cyber-Physical Systems Security (CPSSEC), Cyber Risk Economics (CyRiE), Smart Cities, Transition to Practice (TTP), Mobile Security R&D, and Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT).

Mr. Balenson is co-leading the Platform for Innovative use of Vehicle Open Telematics (PIVOT) project, a coordinated effort to bring together a community around the development and sharing of robust automotive datasets to foster and support new, open cybersecurity research in smart city, transportation, and automotive applications.

He is the Co-PI for the NSF Sharing Expertise and Artifacts for Reuse for Cybersecurity Community Hub (SEARCCH) project, which is developing an open collaboration platform to help researchers package, import, locate, understand, and reuse cybersecurity experiment artifacts. He was the Co-PI for the NSF Cybersecurity Experimentation of the Future (CEF) project, a community-based effort to study current and expected cybersecurity experimentation infrastructure, and to produce a strategic plan and roadmap for developing infrastructure to support future research.

Mr. Balenson has worked for industry leaders including the Johns Hopkins University Applied Physics Laboratory (JHU/APL), SPARTA, McAfee/Network Associates, and Trusted Information Systems. At JHU/APL he was the CONOPS Lead for their National Cyber Range (NCR) Phase II effort. At SPARTA he managed the operational and fiscal activities of their Security Research Division, which conducted fundamental and applied R&D and prototype development for DARPA, DHS, and other government customers; and he was the industry co-lead for Tactical Information Protection technical area from 2001 to 2009 on Army Research Labs (ARL) Collaborative Technology Alliance (CTA) on Communications and Networks. At McAfee Research he helped direct advanced cyber security research, business development, marketing, and technology transfer activities.

He is on the organizing committees for the Annual Computer Security Applications Conference (ACSAC), Network and Distributed Systems Security (NDSS) symposium, IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection (ICCIP), Learning from Authoritative Experiment Results (LASER) workshop, Usable Security (USEC) workshop, and Automotive and Autonomous Vehicle Security (AutoSec) workshop.

Mr. Balenson has worked as an Associate Professorial Lecturer at The George Washington University. He received his M.S. and B.S. in Computer Science from the University of Maryland, College Park.

CHRONOLOGICAL WORK EXPERIENCE

Mar 2012 - present: Senior Computer Scientist, Infrastructure Security Group (ISG), Computer Science Laboratory (CSL), SRI International

Member of the Infrastructure Security Group (ISG), which seeks to improve the cybersecurity of critical infrastructure systems and networks by tackling the hard problems and obstacles in technology, people, and processes in areas such as energy systems, Internet and telecom, financial systems, and other critical infrastructure areas.

Provide technical, management, and subject matter expert support for the Cybersecurity Research and Technical Execution Support (CRATES) and Cyber Security Research and Development Center (CSRDC) at the Department of Homeland Security (DHS) Science and Technology Directorate (S&T).

- Lead support for the Commercialization Accelerator Program (CAP), which seeks to adapt and leverage federally funded mission-relevant technologies to enhance the operational capabilities of DHS and Homeland Security Enterprise (HSE) end users.
- Help establish and lead support the Automotive Cybersecurity Industry Consortium (ACIC), a partnership between automotive manufacturers and DHS to conduct pre-competitive research, development, testing, and evaluation procedures to improve cybersecurity in automotive vehicles.
- Support the Cybersecurity for Gas & Oil (COGS) program and the Gas Technology Institute (GTI) Operational Technology Development (OTD) Cybersecurity Collaborative, a partnership between natural gas distribution companies and DHS to address cybersecurity issues through a focused outreach and education process and a technology evaluation and transfer initiative.
- Help conduct SRI’s Value Creation Workshop (VCW) for DHS S&T performers and staff. VCW introduces SRI's Five Disciplines of Innovation® and teaches value creation tools.
- Lead support for the Cyber-Physical Systems Security (CPSSEC) program, which works to design, implement, and transition new technologies and tools to cyber-physical systems in critical infrastructure sectors, such as automotive, medical, building controls, energy, and manufacturing.
- Lead support for the DHS S&T and NIST Global City Teams Challenge (GCTC) Smart and Secure Cities and Communities Challenge (SC3) thrust, which addresses how to secure complex device networks against cyber-attacks while using these devices to improve community services.
- Support the Cyber Risk Economics (CyRiE) program, which supported research into the business, legal, technical, and behavioral aspects of the economics of cyber threats, vulnerabilities, and controls.
- Lead support for the Transition to Practice (TTP) program, which seeks to successfully transition federally funded cybersecurity technologies into broader use and create an efficient transition process that will have a lasting impact on the R&D community.
- Lead support for the National Critical Infrastructure Security and Resilience (NCISR) R&D Plan, which identifies national R&D priority areas that inform R&D investments, promote innovation, and guide research activities across the critical infrastructure community. Helped develop original 2015 plan as well as draft proposed 2019 update.
- Secondary support for the Mobile Security R&D program, which worked to accelerate the safe and secure adoption of mobile technology within DHS and the federal government, and for the Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) project, which coordinated and developed real-world data and information-sharing capabilities.

Lead support for the Automotive Cybersecurity Industry Consortium (ACIC), including an Automotive Industry Cybersecurity Adoption Survey designed to help individual companies understand current cybersecurity practices and technology and rank their own against the industry, as well as a series of research modules covering secure open-source software, application of continuous development, software/firmware update mechanisms, device/ECU authentication, and securing OEM APIs for developers. Also facilitate planning for future research projects.

Co-lead the Platform for Innovative use of Vehicle Open Telematics (PIVOT) project, a coordinated effort to bring together a community around the development and sharing of robust automotive datasets to foster and support new, open research in areas with strong societal impact such as smart and connected communities and development of cybersecurity and privacy protections for automotive applications.

Co-lead the Cybersecurity Experimentation of the Future (CEF) project, an effort to promote the design, development, and use of a community-wide framework and the associated tools to support experimental cybersecurity research.

- Co-Principal Investigator for the NSF-funded Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub (SEARCCH) project, which is creating a collaborative, community-driven platform that lowers the barrier to sharing by aiding researchers in packaging, importing, locating, understanding, and reusing experiment artifacts.
- Co-Principal Investigator for the NSF-funded Cybersecurity Experimentation of the Future (CEF) project, a community-based effort to study current and expected cybersecurity experimentation infrastructure and to produce a strategic plan and enabling roadmap intended to catalyze generational advances in experimental cybersecurity research.

Member of the Executive Committee and SRI's Lead Representative for the Institute for Internet Infrastructure Protection (I3P), a consortium of 26 academic research institutions, national laboratories, and nonprofit research organizations that bring intellectual breadth and depth to the analysis of cyber security challenges. The I3P is managed by The George Washington University (GWU) in collaboration with SRI International.

Feb 2010 - Mar 2012: Senior Professional Staff, Cyber Assessments Group (QIA), Asymmetric Operations Department (AOD), The Johns Hopkins University Applied Physics Laboratory (JHU/APL)

Concept of Operations (CONOPS) lead for the DARPA-sponsored National Cyber Range (NCR) Phase II prototype effort. Prepared and delivered CONOPS describing planned operation of JHU/APL's Cyber Measurement and Analysis Center (CMAC) prototype during Phase IIB, including overview, organization and staffing plan, facilities, systems overview, "day in the life" examples, high-level process listing, detailed process descriptions, procedure catalog, canonical experiment descriptions, and glossary. Proposal Manager for JHU/APL's NCR Phase IIB proposal.

Project Manager for DARPA/I2O Social Preparation of the Battlespace (SPB) project, which defined challenges and potential solutions to the use of social media in the context of U.S military efforts.

Provide test support for DARPA/TTO System F6 program, which is developing wirelessly networked, resource-sharing clusters of "fractionated" satellites to replace monolithic satellites.

Proposal manager for JHU/APL Scientific Exploration of the Impact Of Social Media within Information Campaigns (SEISMIC) in response to DARPA/I2O Social Media in Strategic Communication (SMISC) BAA 11-64.

Provide R&D coordination support for Research and Standards Integration (RSI) group within the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). Advise team developing DHS Assistant for Research and development Tracking and Technology Transition (DART3), a web-based tool to match and guide transition of federally funded R&D projects meeting DHS requirements.

2005 - 2010: Division Manager, Security Research Division, SPARTA, Inc.

Manage division of principal investigators, research scientists, computer scientists, developers and engineers conducting fundamental and applied R&D and prototype development to fill technology gaps for government and commercial customers.

Focus on information assurance, combined with computer network operations and intelligence. Areas include host security, network security, wireless security, malicious code defense, high-performance assurance and forensics, infrastructure protection, protocol analysis, vulnerability analysis, penetration testing, data collection and analysis, data fusion and understanding, and information sharing. Manage the operational and fiscal activities of the division. Responsible for contract performance, personnel management, technical oversight, business development, and financial budgeting and control.

Team lead for SPARTA's National Cyber Range (NCR) Phase I effort for the Defense Advanced Research Projects Agency (DARPA). Led sub-teams that developed portions of Concept of Operations (CONOPS) and Detailed Engineering Plan (DEP). Led team that developed System Demonstration Plan (SDP). Technical Proposal Manager for SPARTA's NCR Phase I proposal.

Industry co-lead for Tactical Information Protection technical area from 2001 to 2009 on Army Research Labs (ARL) Collaborative Technology Alliance (CTA) on Communications and Networks, researching and developing technologies that enable a fully mobile, fully communicating, agile, situation-aware, and survivable lightweight force with secure, internetted C4ISR systems.

2003 - 2005: Deputy Director, McAfee Research, McAfee, Inc.
2000 - 2003: Director of Technical Outreach, McAfee Research, McAfee, Inc.
(McAfee Research was acquired by SPARTA, Inc. in 2005.)

Oversee research, business development, marketing, and technology transfer activities for advanced information security research laboratory with 50 professionals and staff (50% with advanced degrees) who perform basic and applied research for the United States government, including Defense Advanced Research Projects Agency (DARPA), US Air Force, Army, and multiple intelligence agencies, as well as several major commercial clients in high technology. Areas include host security, network security, wireless security, malicious code defense, high-performance assurance and forensics, infrastructure protection, protocol analysis, vulnerability analysis, penetration testing, data collection and analysis, data fusion and understanding, and information sharing. Manage the operational and fiscal activities of the division. Responsible for contract performance, personnel management, technical oversight, business development, and financial budgeting and control.

1998 - 1999: Manager, Cryptographic Technologies Research Group, Network Associates Laboratory, Network Associates, Inc.
(Network Associates, Inc. rebranded itself as McAfee, Inc. in 1999.)

Manage and direct applied cryptographic technologies research group working to develop, evaluate, and apply cryptographic technologies to satisfy government and commercial information security needs. Responsibilities include initiating and performing externally funded R&D projects, coordinating internal R&D projects, and directing the group's technical staff.

Major DARPA-funded cryptographic technology research projects include:

- Adaptive Cryptographically Synchronized Authentication (ACSA), which developed high-speed authentication techniques for ultra-fast networks by adaptively trading off security & performance; and
- Dynamic Cryptographic Context Management (DCCM), which developed policy-based cryptographic security management techniques and novel One-way Function Tree (OFT) group keying scheme for very large, dynamic group communications.

1996 - 1998: Principal Computer Scientist, Trusted Information Systems, Inc.
(Trusted Information Systems, Inc. was acquired by Network Associates, Inc. in 1998.)

Lead and conduct applied R&D projects involving the design, analysis, implementation, and/or testing of Information Security (INFOSEC) systems employing embedded cryptographic-based Communications Security (COMSEC) solutions.

- Project leader for International Cryptography Experiment (ICE), an informally structured program to advance the general understanding of cryptographic APIs (CAPIs) and their use to promote international cryptography.
- Project leader for Incorporation of Fortezza PCMCIA crypto card into TIS Gauntlet Internet firewall and TIS MIME Object Security Services (TIS/MOSS) software.
- Conduct comprehensive survey of worldwide manufacture and distribution of cryptographic products (1993-2001).
- Principal contributor to design, development, and patenting of Commercial Key Escrow (CKE) and Software Key Escrow (SKE) schemes.

1994 - 2004: Associate Professorial Lecturer, The George Washington University.

Adjunct faculty teaching graduate-level courses on cryptography, network security, and advanced computer security research topics.

1988 - 1996: Computer Scientist, Trusted Information Systems, Inc.

Conduct applied R&D projects involving the design, analysis, implementation, and/or testing of Information Security (INFOSEC) systems employing embedded cryptographic-based Communications Security (COMSEC) solutions.

- Project leader for Air Force Rome Labs (AFRL) effort to develop enhancements for secure distributed operating system, including provisions for cryptographic-based network communications security services.
- Project leader for effort to design, develop and deploy software implementing the Internet Privacy Enhanced Mail (PEM) protocols and infrastructure.
- Project leader for related ARPA-sponsored effort to incorporate a NIST-developed public key smart card into the TIS/PEM software.
- Representative to Internet Privacy and Security Research Group (PSRG), which developed the PEM specifications and designed and analyzed the security for other Internet protocols.
- Coordinator and technical editor for NIST effort to develop draft revised *FIPS 140-1 standard (formerly Federal Standard 1027), General Security Requirements for Cryptographic Modules*.

1984 - 1988, Computer Scientist, Security Technology Group, National Institute of Standards and Technology (NIST)

Participate in the development of Federal and commercial computer security standards and in the research, development and programming of new and advanced methods and techniques for cryptographic security and cryptographic key management protocols.

- Design, implement, and test software implementing NBS cryptographic security standards and ANSI X9E9 Wholesale Financial Services standards.
- Design, implement, and test remote automated validation/conformance-testing tools for ANSI Wholesale Financial Services standards.
- Contribute to the development of ANSI X9E9 Wholesale Financial Services key management (X9.17), authentication (X9.9), and encryption (X9.23) standards.
- Develop and maintain group laboratories including the design, procurement, installation, configuration, testing, programming, and maintenance of experimental and operational hardware/software systems.
- Representative to Internet Privacy Task Force (PTF). Help develop Privacy Enhancement for Internet Electronic Mail RFCs and design, implement, and test software to implement the RFCs using symmetric key management procedures.

Recipient of *1987 United States Department of Commerce Bronze Medal Award* for Superior Federal Service. Cited for the development and implementation of new methods for testing the conformance of vendor devices to Federal and commercial data authentication standards.

EDUCATION

M.S. Computer Science, University of Maryland, 1985. Thesis: *Automated Distribution of Cryptographic Keys*, November 25, 1985. Advisor: Professor Harold P. Edmundson (deceased).

B.S. Computer Science, University of Maryland, 1983.

MAJOR PUBLICATIONS

Terry Benzel, Jelena Mirkovic, Laura Tinnel, David Balenson, Eric Eide, Tim Yardley, Poster: Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub (SEARCCH), Annual Computer Security Applications Conference (ACSAC 2021), December 8, 2021.

Ellis T., Balenson D., Locasto M. (2022) Cyber Security Awareness Requirements for Operational Technology Systems. In: Staggs J., Shenoi S. (eds) Critical Infrastructure Protection XV. ICCIP 2021. IFIP Advances in Information and Communication Technology, vol 636. Springer, Cham.

Terry Benzel, Jelena Mirkovic, Laura Tinnel, David Balenson, Eric Eide, and Tim Yardley, Poster: Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub (SEARCCH), The Network and Distributed System Security Symposium (NDSS 2021), February 21-25, 2021.

Ellis T., Locasto M., Balenson D. (2020) Cyber State Requirements for Design and Validation of Trust in the Critical Transportation Infrastructure. In: Staggs J., Shenoi S. (eds) Critical Infrastructure Protection XIV. ICCIP 2020. IFIP Advances in Information and Communication Technology, vol 596. Springer, Cham.

Terry Benzel, Jelena Mirkovic, Laura Tinnel, David Balenson, Eric Eide, and Tim Yardley, Poster: Sharing Expertise and Artifacts for Reuse through Cybersecurity Community Hub (SEARCCH), 41st IEEE Symposium on Security and Privacy, May 18-20, 2020.

Locasto M., Balenson D. (2019) A Comparative Analysis Approach for Deriving Failure Scenarios in the Natural Gas Distribution Infrastructure. In: Staggs J., Shenoi S. (eds) Critical Infrastructure Protection XIII. ICCIP 2019. IFIP Advances in Information and Communication Technology, vol 570. Springer, Cham.

Erin Kenneally, Lucien Randazzese and David Balenson, "Cyber Risk Economics Capability Gaps Research Strategy," 2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Glasgow, 2018, pp. 1-6.

Douglas Maughan, David Balenson, Ulf Lindqvist, and Zachary Tudor, "Government-Funded R&D to Drive Cybersecurity Technologies," in IT Professional, vol. 17, no. 4, pp. 62-65, July-Aug. 2015.

David Balenson, Laura Tinnel, and Terry Benzel, Cybersecurity Experimentation of the Future: Catalyzing A New Generation of Experimental Cybersecurity Research, Final Report, July 31, 2015.

Bincy Ninan-Moses, Roland Stephen, Lucien Randazzese, Jeffrey Alexander, David Balenson, Ulf Lindqvist, and Zachary Tudor, SRI International Work on Cybereconomic Incentives for the Department of Homeland Security Science and Technology Directorate Cyber Security Division, SRI International, January 31, 2015.

Douglas Maughan, David Balenson, Ulf Lindqvist, and Zachary Tudor, "Crossing the 'Valley of Death': Transitioning Cybersecurity Research into Practice," IEEE Security & Privacy Magazine, Vol. 11, No. 2, March/April 2013, pp. 14-23.

Tom Longstaff, David Balenson, and Mark Matties, "Barriers to Science in Security," In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10), 2010, pp. 127-129.

Dan Sterne, David Balenson, Simon Tsang, Petros Mouchtaris, Maitreya Natu, and Adarshpal Sethi, "Integrating Intrusion Detection and Fault Localization in MANETS," In Proceedings of Military Communications Conference (MILCOM), 2006.

Jamison M. Adcock, David M. Balenson, David W. Carman, Michael Heyman, and Alan T. Sherman, "Trading Off Strength and Performance in Network Authentication: Experience with the ACSA Project," In Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX), 2000, vol. 1, pp. 127-139.

Peter T. Dinsmore, David M. Balenson, Michael Heyman, Peter S. Kruus, Caroline D. Scace, and Alan T. Sherman, "Policy-Based Security Management for Large Dynamic Groups: An Overview of the DCCM Project," In Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX), 2000, vol. 1, pp. 64-73.

Dennis K. Branstad and David M. Balenson, "Policy-Based Cryptographic Key Management: Experience with the KRP Project," In Proceedings of DARPA Information Survivability Conference and Exposition (DISCEX), 2000, vol. 1, pp. 103-114.

David Balenson and Tom Markham, "ISAKMP Key Recovery Extensions," Computers & Security, vol. 19, no. 1, 1 January 2000, pp. 91-99.

Lance J. Hoffman, David M. Balenson, Karen A. Metivier-Carreiro, Anya Kim, and Matthew G. Mundy, "Growing Development of Foreign Encryption Products in the Face of U. S. Export Regulations," The George Washington University Cyberspace Policy Institute, Report GWU-CPI-1999-02 (June 1999). http://cryptome.org/cpi-survey.htm

Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, and David M. Balenson. "Commercial Key Recovery," Communications of the ACM, vol. 39, no. 3 (March 1996), pp. 41-47.

David M. Balenson, "Automated Distribution of Cryptographic Keys Using the Financial Institution Key Management Standard," IEEE Communications Magazine, IEEE, vol. 23, no. 9, pp.41-46, September 1985.

NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995.

US National Standards for Computer Security Technologies, Handbook of Information Security Management: 1994-95 Yearbook, Auerbach Publications, 1994.

Security Requirements for Cryptographic Modules, FIPS 140-1, National Institute of Standards and Technology, Gaithersburg, MD, January 1994.

Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers, Request for Comments (RFC) 1423, Privacy and Security Research Group and Internet Engineering Task Force PEM Working Group, February 1993.

Galvin, James M., David M. Balenson, Steve D. Crocker, and Paul C. Clark, Security Issues of a UNIX PEM Implementation, Proceedings of PSRG Workshop on Network and Distributed System Security, San Diego, CA, February 11-12, 1993.

Galvin, James M., and David M. Balenson, Security Aspects of a UNIX PEM Implementation, Proceedings of USENIX UNIX Security Symposium III, Baltimore, MD, September 14-16, 1992, pp. 119-131.

Balenson, D., W. C. Barker, T. Haley, R. Hartmuller, B. Mayer, C. Pfleeger, L. Schaefer, and D. Vechery, User/Terminal Access in the Post 2000 NATO Tactical Environment, TIS Report 336-3, Trusted Information Systems, Glenwood, MD, September 20, 1990.

Balenson, D., W. C. Barker and C. Pfleeger, Operating Systems Support for Integrated Cryptographic Functions, TIS Report 331, Trusted Information Systems, Glenwood, MD, May 22, 1990.

ANSI Standards for Key Protection, in Network Security Techniques for Financial Institutions (Appendix D), Bank Administration Institute, 1990.

Branstad, M., W. C. Barker, P. Cochrane, and D. Balenson, Key Management and Access Control for an Electronic Mail System, Proceedings 12th National Computer Security Conference, Baltimore, MD, October 10-13, 1989.

Smid, M., E. Barker, D. Balenson and E. Haykin, Message Authentication Code (MAC) Validation System: Requirements and Procedures, Special Publication 500 156, National Bureau of Standards, Gaithersburg, MD, May 1988.

ANSI X9.23-1988, American National Standard for Financial Institution Encryption of Wholesale Financial Messages, American Bankers Association, Washington, DC, 1988.

ANSI X9.9-1986, American National Standard for Financial Institution Message Authentication (Wholesale), American Bankers Association, Washington, DC, 1986.

Smid, M., E. Barker, and D. Balenson, The National Bureau of Standards Message Authentication Code (MAC) Validation System, Proceedings of 9th National Computer Security Conference, Gaithersburg, MD, September 15 18, 1986.

PATENTS

System and Method for Controlling Access to a User Secret Using a Key Recovery Field, #6,272,632, Issued Aug 7, 2001.

System and Method for Data Recovery, #5,991,406, Issued Nov 23, 1999.
System and Method for Access Field Verification, #5,956,403, Issued Sep 21, 1999.
System and Method for Controlling Access to a User Secret, #5,745,573, Issued Apr 28, 1998.
System and Method for Access Field Verification, #5,640,454, Issued Jun 17, 1997.
System and Method for Data Recovery, #5,557,765, Issued Sep 17, 1996.
System and Method for Key Escrow Encryption, #5,557,346, Issued Sep 17, 1996.

COMMUNITY ACTIVITIES

Steering Group, Automotive and Autonomous Vehicle Security (AutoSec) Workshop, 2022.

Steering Group, Usable Security (USEC) Workshop, 2021-present.

Treasurer, Annual Computer Security Applications Conference (ACSAC), 2021.

Panels Chair, Annual Computer Security Applications Conference (ACSAC), 2020.

Steering Committee Chair, Annual Computer Security Applications Conference (ACSAC), 2017-present.

General Chair, Annual Computer Security Applications Conference (ACSAC), 2017-2019.

General Chair, IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, 2017-2020.

Reviewer, IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, 2017-2019.

Coach, Atlantic Council Cyber 9/12 Strategy Challenge, I3P Cyber Fellows Team, 2017-2020.

Program Committee, Usenix Workshop on Cyber Security Experimentation and Test (CSET), 2016, 2018-2021.

Steering Group, Internet Society (ISOC) Symposium on Network and Distributed System Security (NDSS), 2015-present.

Publications Chair, Internet Society (ISOC) Symposium on Network and Distributed System Security (NDSS), 2014-present.

Student Conferenceships Chair, Annual Computer Security Applications Conference (ACSAC), 2013-2016.

Treasurer and Local Arrangements Chair, Learning from Authoritative Security Experiment Results (LASER) Workshop, 2013-present.

Program Committee, Learning from Authoritative Security Experiment Results (LASER) Workshop, 2013-2014.

Cyber Security Track Co-Chair, IEEE International Conference for Technologies for Homeland Security (HST), 2011-2013, 2015-2016.

Steering Group, Internet Society (ISOC) Symposium on Network and Distributed System Security (NDSS), 2003-2005.

General Chair, International Association for Cryptologic Research (IACR) Crypto 2001.

Publicity Chair, Internet Society (ISOC) Symposium on Network and Distributed System Security (NDSS), 1999-2002.

Program Committee, Internet Society (ISOC) Symposium on Network and Distributed System Security (NDSS), 1999.

General Chair, Internet Society (ISOC) Symposium on Network and Distributed System Security (NDSS), 1997-1998.

Program Co-Chair, Internet Society (ISOC) Symposium on Network and Distributed Systems Security (NDSS), 1995-1996.

Program Committee, Internet Society (ISOC) Symposium on Network and Distributed Systems Security (NDSS), 1994.

Program Committee, PSRG Workshop on Network and Distributed System Security, 1993.

Member, Internet Research Task Force Privacy & Security Research Group, 1986-2000.

Member, American National Standards Accredited Standards Committee X9E9 Working Group, Security in Wholesale Financial Telecommunications, 1985-1988.

Reviewer, National Computer Security Conference (NCSC), 1988-1994.

Program Committee, National Computer Security Conference (NCSC), 1987-1988.

Internet Research Task Force (IRTF) Privacy and Security Research Group (PSRG) (formerly Internet Privacy Task Force (PTF)), Member, 1986-2000.

PROFESSIONAL ORGANIZATIONS

Institute of Electrical and Electronics Engineers (IEEE), Senior Member, 2021-present.

International Federation for Information Processing (IFIP) Working Group (WG) 11.10 on Critical Infrastructure Protection, Member, 2017-present.

SAE International, Member, 2016-present.

Applied Computer Security Associates (ACSA), Senior Fellow, 2016-present.

USENIX, The Advanced Computing Systems Association, Sustainer Member, 2013-present.

Association for Computing Machinery (ACM), Member, 1992-present.

Institute of Electrical and Electronics Engineers (IEEE), Member, 1992-2020.

International Association for Cryptologic Research (IACR), Member, 1985-2001, 2019-present.