

Implications of Artificial Intelligence for Cybersecurity: A Workshop

Committee

Frederick R. Chang

Chair

Frederick R. Chang (NAE) is the executive director of the Darwin Deason Institute for Cyber Security, the Bobby B. Lyle Centennial Distinguished Chair in Cyber Security, and professor in the Department of Computer Science and Engineering in the Lyle School of Engineering at Southern Methodist University (SMU). He is also a senior fellow in the John Goodwin Tower Center for Political Studies in SMU's Dedman College. Additionally, Chang's career spans service in the private sector and in government including as the former Director of Research at the National Security Agency (NSA). He has served as a member of the Commission on Cybersecurity for the 44th Presidency and as a member of the Computer Science and Telecommunications Board of the National Academies of Sciences, Engineering and Medicine. Chang is a member of the National Academy of Engineering (2016) and he has been awarded the NSA Director's Distinguished Service Medal. Chang received his B.A. from the University of California, San Diego and his M.A. and Ph.D. from the University of Oregon. He also completed the senior executive program at the Sloan School of Management at the Massachusetts Institute of Technology.

Kathleen Fisher

Member

Kathleen Fisher is a professor and the chair of the Computer Science Department at Tufts. Previously, she was a program manager at DARPA where she started and managed the High-Assurance Cyber Military Systems (HACMS) and Probabilistic Programming for Advanced Machine Learning (PPAML) programs, a consulting faculty member in the Computer Science Department at Stanford University, and a principal member of the technical staff at AT&T Labs Research. Kathleen is an Association for Computing Machinery Fellow. She has served as program chair for Programming Language Design and Implementation, Object-Oriented Programming, Systems, Languages & Applications, International Conference on Functional Programming, Commercial Users of Functional Programming, Foundations of Object-Oriented Language, and as general chair for the International Conference on Functional Programming 2015. She is a former Associate Editor for Transactions on Programming Language and Systems and a former editor of the Journal of Functional Programming. Kathleen is a past chair of the ACM Special Interest Group in Programming Languages (SIGPLAN) and past co-chair of CRA's Committee on the Status of Women (CRA-W). Kathleen is a recipient of the SIGPLAN Distinguished Service Award. She is vice chair of DARPA's ISAT Study Group and a member of the board of trustees of Harvey Mudd College.

Kathleen's work involves developing domain-specific languages to make it easier to solve problems in particular domains. Examples include Hancock for stream processing, PADS for data format manipulation, and Forest for filestore management. She also works in the area of program synthesis, which uses search and/or machine learning techniques to generate programs from high-level specifications. Examples include synthesizing high-performance data structure(s) and concurrency control strategies for a given program and workload, inferring data descriptions from example data, and synthesizing lenses for synchronizing data stored in different formats. She is also interested in applying formal methods and other programming language techniques to produce software that is provably functionally correct with the goal of making hacking into systems much harder than it is today. She is currently working on building tools to make it possible to generate domain-specific language implementations and tools from high level specifications. Dr. Fisher received her PhD in computer science from Stanford University.

Eric Horvitz

Member

Eric Horvitz (NAE) is technical fellow and director of Microsoft Research Labs. He has pursued principles and applications of machine intelligence, with a focus on the use of probability and decision theory in systems that learn and reason. Dr. Horvitz has made contributions in automated diagnosis and decision support, models of bounded rationality; machine learning; human-computer collaboration; and human computation and crowdsourcing. His research and collaborations have led to fielded systems in health care, transportation, human-computer interaction, robotics, operating systems, networking, and aerospace. Dr. Horvitz has been awarded the Feigenbaum Prize and the AAAI-Association for Computing Machinery (ACM) Allen Newell Award for contributions to artificial intelligence and human-computer interaction. He has been elected fellow of the AAAI, the ACM, the American Academy of Arts and Sciences, and the NAE, and he has been inducted into the CHI Academy. Dr. Horvitz earned Ph.D. in biomedical informatics and M.D. at Stanford University.

Subbarao Kambhampati

Member

Subbarao Kambhampati (Rao), is Professor of Computer Science & Engineering at Arizona State University. He joined ASU in 1991, was promoted to Associate Professor in 1996, and Professor in 2000. Prior to joining ASU, he was a research associate with the Center for Design Research and the Department of Computer Science at Stanford University. Rao's research interests are in Artificial Intelligence with particular emphasis on planning, machine learning, analogical and case-based reasoning, and their applications to automated manufacturing. Rao is the recipient of a three-year NSF research initiation award in 1992 and a five-year NSF Young Investigator award in 1994. He currently serves as the president of the Association for the Advancement of Artificial Intelligence (AAAI). He completed his B.Tech. in electrical engineering at Indian Institute of Technology, Madras, India, in 1983. He received his M.S. (1985) and Ph.D. (1989) degrees in computer science from University of Maryland, College Park.

Wenke Lee

Member

Wenke Lee is a professor and John P. Imlay Jr. Chair in the College of Computing at Georgia Tech. He also serves as the director of the Georgia Tech Information Security Center (GTISC). Dr. Lee works in systems and network security. His current research projects are in the areas of botnet detection and attribution; malware analysis; virtual machine monitoring; mobile phone security; and detection and mitigation of information manipulation on the Internet, with funding from NSF, DHS, DoD, and the industry. Dr. Lee has published over 100 articles with more than 40 of them cited more than 100 times. In 2006, Dr. Lee co-founded Damballa, Inc., a spin-off from his lab that focuses on botnet detection and mitigation. He received his Ph.D. in computer science from Columbia University in 1999.

John L. Manferdelli

Member

John Manferdelli is 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, 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.

Phil Venables

Member

Phil Venables is the Chief Information Risk Officer at Goldman Sachs. He leads the Information Security, Technology Risk, Technology Governance and Business Continuity programs. He joined the firm as a vice president in London in 2000 and transferred to New York in 2001. Phil was named managing director in 2003, and partner in 2010. Prior to joining the firm, Phil was Chief Information Security Officer at Deutsche Bank. He also functioned as the global head of Technology Risk Management for Standard Chartered Bank. Prior to that, Phil served in various technology, network management, and software engineering roles at a number of finance, energy, and defense organizations. Phil serves on the executive committee of the U.S. Financial Services Sector Coordinating Council for Critical Infrastructure Protection and the Board of Referees of the journal Computers & Security and is a member of the boards of the Center for Internet Security and the NYU Polytechnic School of Engineering. He is also an advisor to the cyber-security efforts of the U.S. National Research Council, the Institute of Defense Analyses and a U.S. intelligence agency. He was awarded the designation of Chartered Engineer in 1995, Chartered Scientist in 2002, and was elected a fellow of the British Computer Society in 2005. Phil is a member of the Council on Foreign Relations. Phil earned a B.S. (Hons) in computer science from York University in the United Kingdom and an M.S. in computation and cryptography from The Queen's College at Oxford University.

Emily Grumbling

Staff Officer