Workshop on Secure Building Blocks for Trustworthy Systems

National Academies of Sciences, Engineering, and Medicine

UW School of Law, William H. Gates Hall,

Toni C. Rembe Appellate Courtroom

July 31, 2024

Forum on Cyber Resilience - Proprietary

MEETING AGENDA

Workshop on Secure Building Blocks for Trustworthy Systems

Forum on Cyber Resilience

****All sessions are open to the public--** Please register to participate!

Wednesday, July 31, 2024 -- All times US PACIFIC (PDT)

8:00 – 8:30 **BREAKFAST**

8:30 – 8:35 **Welcome**

Tadayoshi Kohno, University of Washington

John Manferdelli, Chair, Forum on Cyber Resilience

Brad Martin, National Security Agency

8:35 – 9:00 **Invited talk** - *Stage setting: Back to the building blocks*

Anjana Rajan, White House Office of the National Cyber Director

9:00 – 10:30 **Fireside Chats** - *Recent progress and future opportunities in memory safety and formal methods*

(9:00- 9:30) *Software*

Moderator: **Dan Wallach,** DARPA

Speaker: **Matt Erickson**, SpiderOak

(9:30-10:00) *Hardware*

Moderator: **Robert Watson,** University of Cambridge

Speaker: **Richard Grisenthwaite**, Arm

(10:00- 10:30) *Formal Methods*

Moderator: **Patrick Lincoln,** SRI

Speaker: **Byron Cook**, AWS

10:30 – 11:00 **BREAK**

11:00 – 12:30 **Panel 1** - *Sector-specific development and use of building blocks and memory safe technologies*

Moderator: **Tim Booher**, Boeing

Speaker: **Greg Shannon,** Idaho National Laboratory

Sushil Birla, U.S. Nuclear Regulatory Commission

Gabriela Ciocarlie, University of Texas, San Antonio

12:30 – 1:30 **LUNCH**

1:30 – 2:00 **Invited talk** – *A look at the software landscape: Challenges and opportunities*

John Viega, Crash Override

2:00 – 3:30 **Panel 2** - *Industry adoption of memory safe technology*

Moderator: **Jonathan Ring**, ONCD

Speaker: **Alex Rebert,** Google

Tony Chen, Microsoft

3:30 – 4:00 **BREAK**

4:00 – 5:00 **Panel 3** - *Building blocks & DARPA connections*

Moderator: **Anjana Rajan,** ONCD

Speakers: **Dan Wallach,** PM, DARPA TRACTOR program

Howie Shrobe, PM, DARPA CPM program

Brad Martin, PM, DARPA PROVERS program

5:00 – 6:00 **Panel 4** – *Exploring paths forward*

Moderator: **Howie Shrobe**, DARPA

Speakers: **Robert Watson**, University of Cambridge

Jonathan Ring, ONCD

Byron Cook, AWS

6:00 – 7:00 **RECEPTION / ADJOURNMENT**

SPEAKER BIOGRAPHIES

Tadayoshi Kohno is a professor in the Paul G. Allen School of Computer Science & Engineering at the University of Washington, where he is also the Associate Director for Diversity, Equity, Inclusion, and Access. He has adjunct appointments in the Department of Electrical & Computer Engineering, the School of Information, and the School of Law. His research focuses on helping protect the security, privacy, and safety of users of current and future generation technologies. Kohno is a recipient of the Alfred P. Sloan Research Fellowship, the U.S. National Science Foundation CAREER Award, the Technology Review TR-35 Young Innovator Award, and the Golden Goose Award. Kohno has authored more than a dozen award papers, has presented his research to the U.S. House of Representatives, had his research profiled in the NOVA ScienceNOW "Can Science Stop Crime?" documentary and the NOVA "CyberWar Threat" documentary, and is a past chair of the USENIX Security Symposium. Kohno is the co-author of the book Cryptography Engineering, co-editor of the anthology Telling Stories, and author of the novella Our Reality. Kohno co-directs the University of Washington Computer Security & Privacy Research Lab and the Tech Policy Lab. Kohno was a founding member of the National Academies Forum on Cyber Resilience and is currently a member of the USENIX Security Steering Committee. Kohno received his Ph.D. from the University of California at San Diego.

John Manferdelli, chair of the forum on cyber resilience, is an independent consultant. Before that, he was, 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.

Brad Martin is the Technical Director for NSA's Laboratory for Advanced Cybersecurity Research. Mr. Martin has a strong history in the area of high confidence software and systems research and development, having initiated research groups at NSA supporting development of scientific foundations and technologies for innovative systems design, systems and embedded application software, and assurance and verification to enable the routine production of reliable, robust, safe, secure, and certifiably dependable IT-centric physical and engineered systems. Mr. Martin serves as Co-Chair of the Networking and Information Technology Research and Development (NITRD) Program's Computing-Enabled Networked Physical Systems (CNPS) Interagency Working Group (IWG). The CNPS IWG coordinates Federal R&D to advance and assure information technology-enabled systems that integrate the cyber/information, physical, and human elements. Additionally, Mr. Martin previously served as the Chair of the Special Cyber Operations Research and Engineering (SCORE) Subcommittee, a Subcommittee of the NSTC Committee on Homeland

& National Security. The SCORE Subcommittee is focused on enhancing coordination and collaboration across the classified cyber research community, and specifically scoped for science and technology for national security needs in cyber.

Anjana Rajan is a cryptographer, technology entrepreneur, and policymaker who works at the nexus of national security and human rights. She currently is the Assistant National Cyber Director for Technology Security at The White House. In this political appointment at the Office of the National Cyber Director, Anjana leads efforts to apply the President's National Cybersecurity Strategy to real world issues, such as open-source software, generative AI, and space. She is the author of ONCD's seminal technical report, "Back to the Building Blocks: A Path Toward Secure and Measurable Software." Previously, Anjana was the first Chief Technology Officer of Polaris, the largest anti-human trafficking NGO in the United States. She was the Chief Technology Officer and co-founder of Callisto, a venture-backed social enterprise that builds advanced cryptographic technology to combat sexual assault. She began her career at Palantir, working in their forward-deployed engineering organization across Europe and the Middle East. Anjana was a Knight Scholar at Cornell University's Engineering School and received her bachelor's and master's degrees in operations research & information engineering. Anjana was a former elite triathlete who raced for Team USA at two world championships.

Dan Wallach is a program manager in DARPA's Information Innovation Office (I2O). He joined DARPA in June 2023 to develop, execute, and transition programs in computer security, cryptography, and related applications. Wallach joined DARPA from Rice University's computer science department, where he works on a variety of topics in computer security, including smartphones and electronic voting systems. Wallach was on the Elections Assistance Commission's Technical Guidelines Development Committee as the IEEE representative (2019-2023), has served as a member of the Air Force Science Advisory Board (2011-2015), and was on the board of directors of the USENIX Association (2011-2012). He was also the lead principal investigator of the National Science Foundation-funded A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections (ACCURATE, 2005-2011). Wallach holds a doctorate and Master of Arts in computer science from Princeton University and a Bachelor of Science from the University of California, Berkeley.

Matt Erickson is the Vice President of Solutions at SpiderOak, a leading company in secure communications and space cybersecurity. Since joining SpiderOak in 2010, he has been pivotal in expanding the company's blockchain and zero-trust technologies for federal clients, particularly within the Department of Defense and intelligence sectors. In this role, he focuses on securing sensitive data and communications in hybrid space environments. In 2018, Matt also served as the Executive Director of the Digital Privacy Alliance, where he advocated for user privacy across the tech industry. His work emphasizes the integration of modern encryption systems and cybersecurity measures in defense and intelligence operations.

Robert Watson is a professor specializing in Systems, Security, and Architecture at the University of Cambridge Computer Laboratory. He is active in several research groups within the lab, with a focus on Security, Networks and Operating Systems, and Computer Architecture. He leads a variety of cross-layer research projects that span computer architecture, compilers, program analysis, program transformation, operating systems, networking, and security. As a strong proponent of open-source software, Robert is on the board of directors for the FreeBSD Foundation and has made notable contributions to the FreeBSD Project. He coauthored the second edition of "The Design and Implementation of the FreeBSD Operating System," published by Pearson. After two and a half years of post-doctoral research at the Computer Laboratory and completing a Research Fellowship at St John's College, Cambridge, in May 2013, he started his lectureship in the department. Prior to this, he spent six years working in several industry research labs (SPARTA ISSO, McAfee Research, NAI Labs, and Trusted Information Systems), investigating operating systems, networking, and security. His work on operating-system security extensibility during this period became the basis for his PhD dissertation. Dr. Watson received his PhD in Computer Science from the Computer Laboratory in 2011.

Richard Grisenthwaite is chief architect and a fellow at Arm Ltd, Cambridge, CB1 9NJ, U.K. His research interests include computer architecture and microarchitecture. Grisenthwaite received his B.A. degree in electrical and information sciences from the University of Cambridge.

Patrick Lincoln is President of Information and Computing Sciences, and Director of the Computer Science Laboratory of SRI International, where he has worked since 1989. Dr. Lincoln holds a Ph.D. in Computer Science from Stanford University and a B.Sc. in Computer Science from MIT. He has previously held positions at MCC, Los Alamos National Laboratory, and ETA Systems. Dr. Lincoln leads research in the fields of formal methods, computer security and privacy, computational biology, scalable distributed systems, and neurosymbolic systems. He has led multidisciplinary groups to high-impact research projects including symbolic systems biology, scalable anomaly detection, exquisitely sensitive biosensor systems, strategic reasoning and game theory, and privacy-preserving data sharing. Dr. Lincoln has published over a hundred influential (cited more than 10 times) papers, has dozens of patents, and has served on scientific advisory boards for private and publicly-held companies, nonprofits, and government agencies and departments.

Byron Cook is Professor of Computer Science at University College London (UCL) and Director of Automated Reasoning at Amazon Web Services. Byron's interests include computer/network security, program analysis/verification, programming languages, theorem proving, logic, hardware design, operating systems, and biological systems. Byron is the founder and leader of Amazon's Automated Reasoning Group (ARG).

Timothy (Tim) Booher is Vice President of Corporate Strategy and Strategic Initiatives at Boeing Company, a role he has held since 2023. Most recently, he served as Vice President of Combat Systems at Lockheed Martin Corporation. Previously, Booher was Chief Technology Officer of Cyber at HSBC Holdings plc. Prior to that role, he served in senior IT and cybersecurity leadership roles at Colgate-Palmolive Company and the US Department of Defense. Earlier in his career, Booher has held various roles at Polco, US Air Force, MIT Active Materials and Structures Lab and Mathsoft Engineering & Education. He began his career in 1997, as a Software Developer at Star Legal. Booher earned a BS in Aeronautical and Astronautical Engineering from Massachusetts Institute of Technology, an MA in Theology Reformed Theological Seminary and an MS in Operations Research from US Air Force Institute of Technology.

Greg Shannon is an Idaho National Laboratory (INL) Fellow and INL's Chief Cybersecurity Scientist – leading strategic approaches to advance scientific methods, cultivate research in emerging technologies, mentor researchers, and advance national and international solutions, all to protect our nation's critical infrastructures from serious cyber-physical threats. Greg joined INL in 2021 from Carnegie Mellon University having served as the Chief Scientist for the CERT Division (originally the Computer Emergency Readiness Team) within the university's Software Engineering Institute. While there, Greg served at the White House Office of Science and Technology Policy as the Assistant Director for Cybersecurity Strategy. In addition to his INL roles, Greg currently serves as: A founding board member and passionate advocate for the Women in Cybersecurity professional society that supports women pursuing careers in cybersecurity; The Chief Science Officer for the Department of Energy's Cybersecurity Manufacturing Innovation Institute (CyManII.org) operated by the University of Texas at San Antonio; and a member of the Department of the Air Force Science Advisory Board. Greg received a B.S. in Computer Science from Iowa State University and a Ph.D. in Computer Sciences at Purdue University.

Sushil Birla is a Senior Technical Advisor at the U.S. Nuclear Regulatory Commission, performing regulatory research for digital safety systems — for example, developing the technical basis for safety evaluation. Formerly, he was a Technical Fellow with General Motors Research and Development, where he earned the coveted Kettering Award for innovative automation of electrical industrial control circuit design. He holds a PhD in Computer Engineering from the University of Michigan, Ann Arbor.

Gabriela F. Ciocarlie is an associate professor in the Department of Electrical and Computer Engineering at The University of Texas at San Antonio and Vice President for Securing Automation and Secure Manufacturing Architecture for CyManII. Her expertise is in anomaly detection, distributed alert correlation, network and application-level security, cyber physical systems security and distributed system security. Before UTSA, Gabriela was the Chief Product Officer at Elpha Secure and a senior technical manager of SRI's New York City research hub focused on cyberanalytics, which she established in 2016. Gabriela was a principal investigator for the DARPA's Transparent Computing program, ARL's Internet of Battlefield Things program, and on multiple commercial and Department of Homeland Security projects focusing on performance degradation detection and causal analysis for mobile broadband networks, anomaly detection for industrial control systems, cyber insurance and accountable clouds. Prior to joining SRI, Gabriela was a senior security research engineer at Real-Time Innovations where she worked on new security models for large-scale distributed systems with real-time and quality-of-service requirements. Gabriela holds a Ph.D. and an M.S. in computer science from Columbia University, and a B.Eng. in computer engineering from Polytechnic University of Bucharest.

John Viega is CEO and Co-founder at Crash Override. Before this, John served as the CEO of Capsule8 from 2016 to 2022. He is a prominent figure in the field of computer science and security, with a career marked by diverse roles and significant contributions to the industry. In addition to his executive roles, John has been an Adjunct Professor of Computer Science at the NYU School of Engineering since 2014, sharing his expertise with the next generation of computer scientists. John's career includes a tenure at BAE Systems Applied Intelligence, where he was the Executive Vice President focusing on Product Management and Engineering for commercial solutions. From 2010 to 2014, he was the Executive Vice President of Products, Strategy, and Services at SilverSky, which was later acquired by BAE Systems. John has also held influential editorial and advisory positions. He was the Editor in Chief of IEEE Security and Privacy Magazine from 2011 to 2012 and served on the Technical Advisory Board at Fortify Software from 2007 to 2011. His earlier career included roles at McAfee, Bit9, and Stonewall Software. John's extensive experience and contributions to the field underscore his status as a leading expert in computer science and security. His formative education took place at Wakefield School, where he studied from 1984 to 1991. John also holds a Pragmatic Marketing Certified - Level VI (PMC-VI) credential from Pragmatic Marketing, although the specific date of certification is not noted. He earned a Bachelor of Arts degree in 1996 and a Master of Science degree in Computer Science in 1998, both from the University of Virginia.

Jonathan Ring is the Deputy Assistant National Cyber Director for Technology Security at ONCD. He began his tenure at ONCD in 2022, starting as the Director of Operations and Incident Response. With more than a decade of experience, Jonathan has led teams to tackle complex technical and organizational challenges and has formulated cybersecurity policies for supply chain, AI, and advanced threat actors. He earned a Master of Law and Technology from Georgetown University Law Center and holds bachelor's degrees in information sciences and technology and security and risk analysis from Penn State University.

Alex Rebert is an engineer in Google's Information Security Engineering organization, whose goal is to keep Google's products secure and users safe. Alex focuses on memory safety, and recently published Google's perspective on it. Before Google, Alex co-founded ForAllSecure to help companies find unknown vulnerabilities, where he led the team that created Mayhem, an autonomous agent that could find, exploit, and patch vulnerabilities. Mayhem won the DARPA Cyber Grand Challenge in 2016. Alex was named one of MIT Tech Review's 35 Innovators Under 35 and Forbes' 30 Under 30.

Tony Chen is a software engineer and security architect at Microsoft. Tony has worked at Microsoft since 1997 and is currently a Partner Security Architect in the OS Security team. Since joining Microsoft, Tony has spent most of his career working on Xbox. He was a founding member of the Xbox Live team since 2000 and contributed to the launch of Xbox Live in 2002 and its continued growth through 2011. Starting in 2011, Tony worked on security for Xbox to prevent cheating and piracy. He worked with the Microsoft hardware team and AMD to successfully design and launch the Xbox One game console in 2013 which to this day still has not been hacked to enable piracy and cheating. It is the only game console ever made to have such a long record of upholding security. Since 2014, Tony has been working in the OS Security team to help improve the security of Windows devices through a combination of hardware and software changes. In recent years, Tony has taken interest on how to combat memory safety issues and has pushed for the usage of CHERI based microprocessor cores to enhance security of modern SoCs. Dr. Chenn graduated from National Taiwan University Electrical Engineering Department in 1986 and received a Ph.D. in Computer Science from University of Maryland at College Park in 1992.

Howie Shrobe is a program manager in the Information Innovation Office (I20) at DARPA. He previously served as a principal research scientist at MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL). He joined the MIT AI Lab (which later joined with the Lab for Computer Science in forming CSAIL) in 1978. He leads the Software Defined Hardware (SDH), Machine Common Sense (MCS), Compartmentalization and Privilege Management (CPM) and the Machine-learning and Optimization guided Compilation for Heterogenous Architectures (MOCHA) programs. He previously served at DARPA in the Information Technology Office from 1994 – 1997 where he initiated the Information Survivability initiative and from 2010 – 2013 in I2O where he led the Clean-slate design of Resilient and Secure Hosts (CRASH) and Mission-oriented Resilient Clouds (MRC) programs. His interests include hardware and software approaches to inherently secure systems and AI. Dr. Shrobe received his BS from Yale college in 1968 and his MS and PhD from MIT's Electrical Engineering and Computer Science Department in 1975 and 1978 respectively.

FORUM ON CYBER RESILIENCE ROSTER

John L. Manferdelli, Chair
Independent Consultant
Email: johnmanferdelli@hotmail.com

Heather Adkins
Office of Cybersecurity Resilience
Google, Inc.
Email: argv@google.com

Yair Amir
Professor
Johns Hopkins University
Email: yairamir@cs.jhu.edu

Hyrum Anderson
CTO
Robust Intelligence
Email: hyrum@robustintelligence.com

Steven M. Bellovin, NAE
Percy K. and Vida L.W. Hudson Professor
Columbia University
Email: smb@cs.columbia.edu

Thomas A. Berson, NAE
Advisory Board Member
Salesforce
Email: berson@anagram.com

Nadya T. Bliss
Executive Director
Global Security Initiative, Arizona State University
Email: nadya.bliss@asu.edu

Timothy Booher
Vice President of Corporate Strategy and Strategic Initiatives
Boeing
Email: tim.booher@boeing.com

Srini Devadas
Edwin Sibley Webster Prof. of Electrical Engineering & Computer Science
Computer Science and Artificial Intelligence Lab
Massachusetts Institute of Technology
Email: devadas@mit.edu

Paul England, NAE
Distinguished Engineer
Microsoft
Email: paul.england@microsoft.com

Alexander Gantman
VP of Engineering
Qualcomm Technologies Inc.,
Email: agantman@qti.qualcomm.com

James R. Gosler, NAE
Senior Fellow
Johns Hopkins Applied Physics Laboratory
Email: jrgosler@gmail.com

Galen Hunt
Distinguished Engineer
Microsoft
Email: galen.hunt@microsoft.com

John C. Inglis
Professor for Cyber Studies
U. S. Naval Academy Looker Distinguished Visiting Professor
Email: Inglis@usna.edu

Brian LaMacchia
Executive Director
MPC Alliance
Email: bal@farcaster.com

John Launchbury
Chief Scientist
Galois, Inc.
Email: john@galois.com

Dave Levin
Associate Professor, Computer Science
University of Maryland
Email: dml@cs.umd.edu

Damon McCoy
Professor, Computer Science
New York University Tandon School of Engineering
Email: mccoy@nyu.edu

Sean Peisert
Senior Scientist, Computing Science Research
Lawrence Berkeley National Lab
Email: sppeisert@lbl.gov

Window Snyder
CEO and Founder
Thistle Technologies
Email: window@thistle.tech

Parisa Tabriz
Director of Engineering
Google
Email: parisa@google.com

Ex Officio Members

Jeremy J. Epstein
Program Director
National Science Foundation
Computer and Information Sciences and Engineering
Email: jepstein@nsf.gov

William "Brad" Martin
Technical Director
NSA's Laboratory for Advanced Cybersecurity Research
Email: wbmarti@nsa.gov

Kevin Stine
Director, Information Technology Lab (ITL)
National Institute for Standards and Technology
Email: kevin.stine@nist.gov

Forum Staff

Tho Nguyen, Director, Forum on Cyber Resilience, CSTB
Email: thonguyen@nas.edu

Jon Eisenberg, Senior Board Director, CSTB
Email: jeisenbe@nas.edu

Shenae Bradley, Administrative Coordinator, CSTB
Email: sbradley@nas.edu

Gabrielle Risica, Program Officer, CSTB
Email: grisica@nas.edu

Nneka Udeagbala, Associate Program Officer, CSTB
Email: nudeagbala@nas.edu