CAD for Hardware Security (CAD4Sec) Workshop

CAD FOR SECURITY

59 DESIGN AUTOMATION CONFERENCE

SCAN ME

Wi-Fi Passcode:
59DAC2022

10 July 2022
Moscone West, San Francisco

Keynote Address, Talks, Panel, and Demo

59 DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Keynote Address

Jay Lewis
DC Site Lead of Silicon Security
Microsoft Corporation

Invited Talks

Norman Chang
Chief Technologist
ANSYS Inc.

Dan Walters
Principal Embedded Security Engineer
MITRE

Jason Oberg
Co-Founder and CTO
Cycuity

Jeremy Bellay
Principal Research Scientist
Battelle

Mike Borza
Principal Security Technologist
Synopsys

Dan Benua
Director of Application Engineering
Cadence Design Systems

Nicole Fern
Senior Security Analyst
Riscure

Beau Bakken
Principal Engineer
Caspia Technologies

Ujjwal Guin
Assistant Professor
Auburn University

Hadi M Kamali
Postdoctoral Research Associate
University of Florida

CAD Demos

Caspia Technologies

UF UNIVERSITY of FLORIDA

UNIVERSITY of SOUTH FLORIDA 1956

Panel Discussion

John Goodenough
Tech Leader in SoC Design
Former VP at ARM

Adam Cron
Distinguished Architect
Synopsys

Saverio Fazzari
Senior Lead Engineer
BAH

Adam Kimura
Senior Research Scientist
Battelle Memorial Institute

Sid Allman
Senior Director
Marvell Technology

Keynote Address

59 DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Jay Lewis

DC Site Lead of Silicon Security
Microsoft Corporation

Microsoft

Dr. Jay Lewis is a Partner at Microsoft focusing on technology incubation, and on strategic semiconductor supply chain risks. In the tech incubation role, this means ensuring that new ideas have a path to become the next generation of products and customer capabilities. The supply chain role includes addressing critical risks to the continuity and integrity of the hardware supply chain. Prior to starting at Microsoft in 2020 Jay was the Deputy Director of the Microsystems Technology Office at DARPA, and prior to that was a Program Manager at DARPA. He has published over 35 refereed articles and been awarded more than 10 patents.

Invited Talk #1

DESIGN AUTOMATION CONFERENCE 59

CAD FOR SECURITY

riscure

driving your security forward

Nicole Fern

Senior Security Analyst
Riscure

Nicole Fern is a Senior Security Analyst at Riscure. She received her PhD degree in Electrical & Computer Engineering from University of California, Santa Barbara in 2016 and continued her research in hardware security as a post-doc before joining industry in 2018. She joined Riscure in 2021 and is currently interested in all things embedded security and hardware hacking!

Invited Talk #2

Dan Walters

Principal Embedded Security Engineer
MITRE

Dan Walters is a Principal Embedded Security Engineer and Group Leader at MITRE Labs in the department for Electronics System Development and Embedded Security. Dan helped to develop MITRE's Secure Electronics Lab, which has advanced capabilities for researching implementation security issues such as side-channel leakage, fault induction, and trusted hardware. Dan is also a part-time lecturer at the University of Massachusetts-Amherst where he teaches embedded security topics at the graduate level. He received his M.S. in Computer Science with a focus on machine learning for security applications from Tufts University; and his B.S.E. in Computer Engineering, B.S.E. in Electrical Engineering, and B.S.E. in Mathematics from the University of Michigan.

Visionary Talk

Norman Chang

Chief Technologist
ANSYS

Norman Chang co-founded Apache Design Solutions in February 2001 and currently serves as Ansys Fellow and Chief Technologist of Electronics, Semiconductor, and Optics BU, ANSYS, Inc. He is also currently leading AI/ML and security initiatives at ANSYS. Prior to Apache, he lead a research group on the research of Power/Signal/Thermal Integrity of chipsets based on VLIW architecture at HP Labs. Dr. Chang received his Ph.D. in Electrical Engineering and Computer Sciences from University of California, Berkeley. He holds twenty patents and has co-authored over 60 technical papers and a popular book on “Interconnect Analysis and Synthesis” by Wiley-Interscience at 2000. He is currently in the committee for EDPS, ESDA-EDA and SI2 AI/ML SIG, and an IEEE Senior Member.

Invited Talk #3

59 DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Jeremy Bellay

Principal Investigator
Battelle

BATTELLE
It can be done

Jeremy Bellay, Ph.D. is a principal investigator in Battelle’s Cyber Trust and Analytics division. He specializes in problems that require the synthesis of complex knowledge structures with sophisticated data driven approaches. Jeremy is particularly interested in an integrative approach to risk and assurance in cyber systems. He led the TAME Forum working group on Hardware Assurance, Weaknesses, Collaboration and Sharing. He is currently an active participant in the SAE G32 Hardware Assurance effort and the ICT SCRM HBOM development working group.

Invited Talk #4

59 DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Beau Bakken

Principal Engineer
Caspia Technologies

Caspia Technologies

Beau Bakken is a Principal Engineer at Caspia Technologies leading projects in multiple areas of microelectronic security, including IP protection, fault injection assessment, side-channel analysis, and PCB assurance. He joined Caspia in 2020 and holds a degree in Computer Engineering from the University of Florida.

Invited Talk #5

59 DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Ujjwal Guin

Assistant Professor
Auburn University

Ujjwal Guin (Member, IEEE) received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Connecticut, in 2016. He is currently an Assistant Professor with the Department of ECE, Auburn University. He has developed several on-chip structures and techniques to improve the security, trustworthiness, and reliability of integrated circuits. He has been serving on the technical program committees of several reputed conferences, such as DAC, HOST, VTS, PAINE, VLSID, GLSVLSI, ISVLSI, and Blockchain. He is an active participant in the SAE International G-19A Test Laboratory Standards Development Committee and G-32 Cyber-Physical Systems Security Committee.

Invited Talk #6

59 DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Jason Oberg

Co-Founder and CTO

Cycuity

Cycuity

Dr. Jason Oberg is a co-founder and Chief Technology Officer (CTO) of Cycuity, where he is responsible for overseeing the company's technology and strategic positioning. As a leading expert in hardware security, Dr. Oberg brings years of deep expertise and has facilitated the development of several disruptive hardware security technologies. His work has been cited over 1000 times and he holds seven issued and pending patents. Prior to his CTO role, Dr. Oberg led Cycuity as co-founder and CEO from 2014 – 2020, during which he facilitated raising capital, recruited the initial team, and drove the company's product revenue growth YoY. He received his B.S. in Computer Engineering from UC Santa Barbara and an M.S. and Ph.D. in Computer Science from UC San Diego.

Invited Talk #7

Dan Benua

Director of Application Engineering
Cadence

Daniel Benua is an AE Director at Cadence Design Systems based in San Jose, California. Previously, Daniel was a Principal CAE at Synopsys. Dan is an industry expert in the application of formal technology to hardware design verification problems, and he has rich experiences in verification-based tool support, methodology consulting, training, and product direction.

Invited Talk #8

DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Hadi M Kamali

Postdoctoral Research Associate
University of Florida

UF UNIVERSITY of FLORIDA

Hadi M Kamali is a postdoctoral research associate at Florida Institute for Cybersecurity Research (FICS), the Department of Electrical and Computer Engineering at the University of Florida. He received his Ph.D. degree from the Department of Electrical and Computer Engineering at George Mason University, 2021. His research delves into hardware security with a particular focus on exploiting IP protection techniques, design-for-trust for VLSI circuits, and CAD frameworks for security (design-for-security), in which he has numerous publications in top journals and conferences including IEEE TC/TVLSI/TCAD, IACR Transactions on CHES, DAC, ICCAD, HOST, etc., with awards including nominations/selections for the Best Paper Award in ISVLSI'20, ICCAD'19, ICCAD'20, ISCAS 2021, and HOST 2022.

Panel Discussion

59 DESIGN AUTOMATION CONFERENCE

CAD FOR SECURITY

Secure Silicon Development Lifecycle

Challenges & Solutions

Moderator :

Dr. Farimah Farahmandi
Assistant Professor
University of Florida

John Goodenough
Tech Leader in SoC Design
Former VP at ARM

Adam Cron
Distinguished Architect
Synopsys

Saverio Fazzari
Senior Lead Engineer
BAH

Adam Kimura
Senior Research Scientist
Battelle Memorial Institute

Sid Allman
Senior Director
Marvell Technology

Sohrab Aftabjahani
Senior Staff Security Researcher
Intel Corporation

Panel Questions

- Security signoff versus design signoff – Similarities and differences
- Where do you think the emphasis should be when we establish these solutions?
- What emerging topics will have major impacts in hardware security in next 5-10 years? Digital twins?
- AI/machine learning
- What is the biggest barrier in making security EDA solutions accepted by customers?
- Who are the potential customers/users of these tools?
- What is the role of the industry/government/academia in establishing EDA solutions/Standards/Best practices?
- Where do you think the security EDA will be in next 5 to 10 years?

Closing Thoughts

Mike Borza

Principal Security Technologist
Synopsys

Mike Borza is a member of the technical staff for Synopsys security IP. He has more than 20 years of experience in security system engineering, and safety critical engineering before that. He is a founder and CTO of Elliptic Technologies, which was acquired by Synopsys. Borza has been an active contributor to the Security Task Group of IEEE 802.1; was an editor of the 802.1AR Secure Device Identifier standard; and is one of the founding members of the prpl Foundation and co-chair of its Security Engineering Group. He holds a Master’s Degree in Electrical Engineering from McMaster University.

Thank You

CAD FOR SECURITY

59 DESIGN AUTOMATION CONFERENCE