COMPUTING COMMUNITY CONSORTIUM

CCC

SRC®

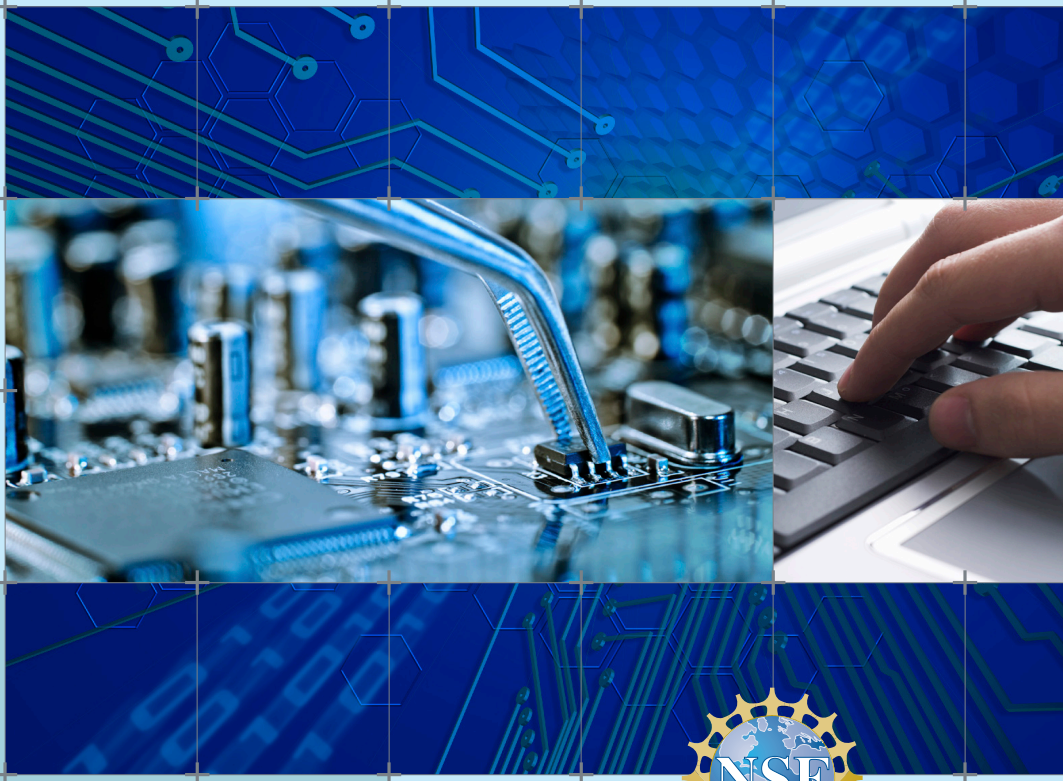
Semiconductor Research Corporation

Convergence of SOFTWARE ASSURANCE Methodologies and TRUSTWORTHY SEMICONDUCTOR Design and Manufacture

SA+TS

www.cra.org/ccc/

www.src.org



NSF

Convergence of
SOFTWARE ASSURANCE Methodologies
and **TRUSTWORTHY SEMICONDUCTOR**
Design and Manufacture

SA+TS

WORKSHOP SUMMARY

In today's electronic world, trustworthy and reliable systems depend on trustworthy and reliable semiconductors. Ensuring that a computer chip or other semiconductor-based component does what is intended—and nothing else—is an increasingly challenging goal.

Semiconductor design and manufacture depends on a "pipeline" of tools and processes, often involving a number of suppliers and customers, with various steps along the way at which the intended product may be altered, either maliciously or inadvertently. Strengthening the tool chain and developing practical and robust approaches to authentication can help to avoid such alterations. The programming language community has, over the last two decades, addressed closely related problems with solutions such as "proof carrying code" and "certifying compilation".

The workshop will bring together academic, industry, and government scientists and engineers from the programming language and semiconductor communities to discuss challenges to securing the semiconductor design and manufacturing pipeline. Interactive sessions will focus on strategies, based in part on experience in the programming language community, for addressing those challenges. A goal of the workshop is to make connections among diverse academic research groups and industry experts and to identify new areas of research aimed at improving trustworthiness and reliability of semiconductors during the design and manufacturing process.

WORKSHOP AGENDA

January 15

	Continental breakfast
8:30 AM	Welcome and Overview of the Workshop • Keith Marzullo, NSF, Director of Computer and Network Systems Division • Workshop Sponsors (Jeremy Epstein, NSF & Celia Merzbacher, SRC)

Plenary Session 1: Overview of Semiconductor Design and Manufacture (with an eye toward the future)

9:00 AM	Moderator – Ron Perez, AMD *Semiconductor Manufacture Tools & Processes and Potential Vulnerabilities (15 mins)—K. Kemp, Freescale* *Semiconductor Design Tools & Processes and Potential Vulnerabilities (15 mins)—S. Trimberger, Xilinx* *Top-to-bottom integrative design & verification (15 mins)—C. Seger, Intel* *Incorporation of designs from multiple sources (15 mins)—R. Aitken, ARM* Panel Discussion (30 mins)
10:30 AM	BREAK

Plenary Session 2: Overview of Software Assurance Methodologies

11:00 AM	Moderator – Fred Schneider, Cornell University *Thinking about attacks / minimizing trusted base (20 mins)—A. Appel, Princeton University* *CompCert as a software tool chain (20 minutes)—D. Pichardie, INRIA/Harvard University* *Specifying the HW/SW interface (20 minutes)—P. Sewell, University of Cambridge* Panel Discussion (30 mins)
12:30 PM	LUNCH *Reality of hardware vulnerability—F. Kiamlev and F. Cayci, University of Delaware*
1:30 PM	Breakout sessions (facilitated discussion on specified questions) Facilitators: Jeremy Epstein (NSF), Fred Schneider (Cornell University) and Yervant Zorian (Synopsys)
5:00 PM	Preliminary Breakout reports (5 min each; bring forward one or two issues/ideas for consideration by all)
6:00 – 8:00 PM	Reception

WORKSHOP AGENDA *CONTINUED*

January 16

	Continental breakfast
8:30 AM	Welcome: Suzanne Iacono, Deputy Assistant Director, Directorate for Computer & Information Science & Engineer, NSF
	Opening remarks: Overview of Day 2 (C. Merzbacher/J. Epstein)

Plenary session 3: Further food for thought

	Moderator – Ruby Lee, Princeton University
8:35 AM	*Counterfeit chips: What are the threats?* *(20 mins + 5 mins Q&A)—M. Tehranipoor, University of Connecticut*
9:00 AM	*Why information flow is different from—and harder than—verifying other kinds of properties* *(20 mins + 5 mins Q&A)—S. Zdancewic, University of Pennsylvania*
9:30 AM	Continue Breakout Groups to finalize output (with 15 min break)
12:00 PM	Breakout Group reports & discussion—Working lunch
1:30 PM	Wrap-up
2:00 PM	Adjourn

WORKSHOP PARTICIPANTS

Rob	Aitken	ARM	rob.aitken@arm.com
Nina	Amla	NSF	namla@nsf.gov
Andrew	Appel	Princeton University	appel@cs.princeton.edu
Kris	Ardis	Maxim Integrated	kristopher.ardis@maximintegrated.com
Clark	Barrett	NYU	barrett@cs.nyu.edu
Sankar	Basu	NSF	sabasu@nsf.gov
Jay	Bhadra	Freescale	jayanta.bhadra@freescale.com
Arnett	Brown	DARPA	arnett.brown.ctr@darpa.mil
Furkan	Cayci	University of Delaware	furkan@udel.edu
Chris	Collins	Texas Instruments	collins@ti.com
Chris	Daverse	SRC	chris.daverse@src.org
Jeremy	Epstein	NSF	jepstein@nsf.gov
Benjamin	Epstein	DARPA	benjamin.epstein.ctr@darpa.mil
Saverio	Fazzari	DARPA	fazzari_saverio@bah.com
Kathleen	Fisher	DARPA	kathleen.fisher@darpa.mil
Alex	Halderman	University of Michigan	jhalderm@eecs.umich.edu
Kenneth	Hines	Computing Community Consortium	khines@cra.org
Suzanne	Iacono	NSF	siacono@nsf.gov
Anupam	Joshi	University of Maryland	joshi@cs.umbc.edu
William	Joyner	SRC	william.joyner@src.org
Ramesh	Karri	NYU	rkarri@duke.poly.edu
Kevin	Kemp	Freescale	rxpg40@freescale.com
Fouad	Kiamlev	University of Delaware	kiamlev@ece.udel.edu
Farinaz	Koushanfar	Rice University	farinaz@rice.edu
Andreas	Kuehlmann	Coverity	akuehlmann@coverity.com
Richard	Kuhn	NIST	dkuhn@nist.gov
Ruby	Lee	Princeton University	rblee@ee.princeton.edu
Patrick	Lincoln	SRI	lincoln@csl.sri.com
Igor	Linkov	US Army Corps of Engineers	igor.linkov@usace.army.mil
Rafic	Makki	GLOBALFOUNDRIES	makki@globalfoundries.com

Brad	Martin	ODNI	wbmarti@tycho.ncsc.mil
Keith	Marzullo	NSF	kmarzull@nsf.gov
Carl	McCants	IARPA	carl.e.mccants@ugov.gov
Celia	Merzbacher	SRC	celia.merzbacher@src.org
Ron	Perez	AMD	ron.perez@amd.com
David	Pichardie	INRIA	david.pichardie@inria.fr
James	Plusquellic	University of New Mexico	plusquel@umbc.edu
Tim	Polk	OSTP	william_t_polk@ostp.eop.gov
Dennis	Polla	IARPA	dennis.l.polla@ugov.gov
Dan	Radack	IDA	dradack@ida.org
Farhan	Rahman	AMD	farhan.rahman@amd.com
Juan	Rey	Mentor Graphics	juan_rey@mentor.com
Fred	Schneider	Cornell University	fbs@cs.cornell.edu
Carl	Seger	Intel	carl.seger@intel.com
Peter	Sewell	University of Cambridge	peter.sewell@cl.cam.ac.uk
Mani	Soma	University of Washington	manisoma@uw.edu
Peilin	Song	IBM	psong@us.ibm.com
Gang	Tan	Lehigh University	gtan@cse.lehigh.edu
Mohammed	Tehranipoor	University of Connecticut	tehrani@engr.uconn.edu
Steve	Trimberger	Xilinx	steve.trimberger@xilinx.com
Vivek	Vedula	Freescale	b35209@freescale.com
Ingrid	Verbauwhede	UCLA & Leuwen	ingrid@ee.ucla.edu
Claire	Vishik	Intel	claire.vishik@intel.com
Bob	Wisnieff	IBM	wisnieff@us.ibm.com
Amanda	Wright	SRC	amanda.wright@src.org
Steve	Zdancewic	University of Pennsylvania	stevez@cis.upenn.edu
Fen	Zhao	OSTP	fen_zhao@ostp.eop.gov
Yervant	Zorian	Synopsys	yervant.zorian@synopsys.com

ORGANIZING COMMITTEE:

Andrew Appel
Princeton University

Chris Daverse
Semiconductor Research Corporation

Kenneth Hines
Computing Community Consortium

Rafic Makki
GLOBALFOUNDRIES

Keith Marzullo
National Science Foundation

Celia Merzbacher
Semiconductor Research Corporation

Ron Perez
Advanced Micro Devices

Fred Schneider
Cornell University

Mani Soma
University of Washington

Yervant Zorian
Synopsys

Established in 2006 through a Cooperative Agreement between the National Science Foundation (NSF) and the Computing Research Association (CRA), the CCC serves as a catalyst and enabler for the computing research community. Its goals are to unite the community to contribute to shaping the future of the field; provide leadership for the community, encouraging revolutionary, high-impact research; encourage the alignment of computing research with pressing national priorities and national challenges (many of which cross disciplines); give voice to the community, communicating to a broad audience the many ways in which advances in computing will create a brighter future; and grow new leaders for the computing research community.

Semiconductor Research Corporation

SRC is a recognized leader in managing collaborative research and has developed efficient, effective and proven mechanisms and processes for creating and managing industry consortia, setting direction, managing and coordinating the research, and disseminating the results. SRC's primary objectives are to support the competitiveness of its company members (individually and collectively), explore new technologies, stimulate industry-relevant academic research, promote greater academic collaboration, and sustain a pool of experienced faculty and a pipeline of relevantly educated students. Since its inception in 1982, SRC has managed over $1.5 billion in basic academic research at more than 200 universities worldwide and supported approximately 10,000 students, who have gone on to become the next generation of leading-edge researchers, technology innovators and industry leaders. Processes and infrastructure developed by SRC identify and communicate industry's collective basic research needs, connect the academic faculty and student researchers with industry "users", support university research with high impact potential, and deliver early results to members.

www.cra.org/ccc/

www.src.org

Semiconductor Research Corporation