

Program Agenda

Tuesday, May 8 – Theme: Technology Transfer

Moderator: *John Launchbury (Galois, Inc.)*

7:30 – 8:30 **Continental Breakfast and Registration**

8:30 – 9:30 **Formal Methods and DO-178C**

Darren Cofer (Rockwell Collins)

9:30 – 10:00 **Refreshments**

10:00 – 10:40 **Accessible Integrated Formal Reasoning Environments in Classroom Instruction of Mathematics**

Andrei Lapets (Boston University)

10:40 – 11:20 **Structured Orchestration of Data and Computation**

Jayadev Misra (University of Texas at Austin)

11:20 – 12:00 **Developer-Friendly Contract-Based Notations and Machine-Checkable Evidence for Verification of Information Flow Properties for Embedded Systems**

John Hatcliff (Kansas State University)

12:00 – 13:30 **Lunch**

13:30 – 14:30 **Keynote: Technology Transfer Challenges within the S&T Community**

Dawn Meyerriecks (ODNI)

14:30 – 15:00 **Refreshments**

15:00 – 15:45 **Tech Transfer of Software Tools**

Jim Larus (Microsoft Research)

15:45 – 16:30 **VehicleForge.mil: A Distributed, Semantically-Aware Framework to Support the Needs of the Open Hardware Community**

Jack Zentner (Georgia Tech)

16:30 – 17:00 **Open Discussion on Technology Transfer**

17:00 Adjourn for the day

Wednesday, May 9 – Theme: Formal Synthesis

Moderator: *Frank Taylor (NSA)*

- 7:30 – 8:30 **Continental Breakfast and Registration**
- 8:30 – 9:30 **Keynote: Program Synthesis for Performance**
Markus Püschel (ETH Zurich)
- 9:30 – 10:00 **Poster Session and Refreshments**
- 10:00 – 10:40 **Preventing Exploits Against Software of Uncertain Provenance**
David Melski (GrammaTech, Inc.)
- 10:40 – 11:20 **VIBRANCE: Automatic Removal of Security Vulnerabilities from Java Applications**
Alessandro Coglio (Kestrel Institute)
- 11:20 – 12:00 **Compositional Verification of Architectural Models**
Darren Cofer (Rockwell Collins)
- 12:00 – 13:30 **Lunch**
- 13:30 – 14:10 **Formal Synthesis of Efficient Verified Emulators**
Magnus Myreen (University of Cambridge, UK)
- 14:10 – 14:50 **Synthesizing Architectural Models of Cyber-Physical Systems**
Pete Manolios (Northeastern University)
- 14:50 – 15:30 **Static Previrtualization**
Natarajan Shankar (SRI, International)
- 15:30 – 16:00 **Poster Session and Refreshments**
- 16:00 – 16:40 **Synthesis of Concurrent Garbage Collectors**
Douglas Smith (Kestrel Institute)
- 16:40 – 17:20 **High Assurance Cyber Military Systems: A New DARPA Program**
Kathleen Fisher (DARPA)
- 17:20 Adjourn for the day
- 18:30 – 20:30 **HCSS Conference Dinner (The Chart House)**

Thursday, May 10 – Theme: Compositional Reasoning

Moderator: *Raymond Richards (Rockwell Collins)*

- 7:30 – 8:30 **Continental Breakfast and Registration**
- 8:30 – 9:30 **Keynote: A New Approach to Temporal Property Verification**
Byron Cook (Microsoft Research)
- 9:30 – 10:00 **Refreshments**
- 10:00 – 10:40 **The Ramification Rule of Separation Logic**
Jules Villard (University College London, UK)
- 10:40 – 11:20 **Verification of Elliptic Curve Cryptography**
Joe Hendrix (Galois, Inc.)
- 11:20 – 12:00 **Axe: An Automated Formal Equivalence Checking Tool for Programs**
Eric Smith (Kestrel Institute)
- 12:00 – 13:30 **Lunch**
- 13:30 – 14:10 **Reasoning About Non-Determinism**
Eric Koskinen (University of Cambridge, UK and New York University)
- 14:10 – 14:50 **FUSE: Inter-Application Security for Android**
Joe Hurd (Galois, Inc.)
- 14:50 – 15:30 **Framework for Evaluating Information Flows in Multicore Architectures for High Assurance Systems**
Ryan Bradetich (University of Idaho)
- 15:30 – 16:00 **Refreshments**
- 16:00 – 16:40 **Software Model Checking Secure Systems**
Limin Jia (Carnegie Mellon University)
- 16:40 – 17:20 **3 Years After L4.verified**
Gerwin Klein (NICTA and UNSW, Australia)
- 17:20 **Adjourn for the day**

Friday, May 6 – Designed-In Security Symposium

Moderator: *Brad Martin (ODNI/ NSA)*

7:30 – 8:30 **Continental Breakfast and Registration**

8:30 – 9:00 **A Brief Introduction to Designed-In Security**

Carl Landwehr (Cyber Security Policy and Research Institute)

9:00 – 10:00 **Keynote: Ensuring System Resilience at Design Time: A User and Attacker Oriented Approach**

William Sanders (University of Illinois Urbana-Champaign)

10:00 – 10:30 **Refreshments**

10:30 – 11:15 **Twenty Years of Industrial Formal Methods**

Steve Miller (Rockwell Collins)

11:15 – 12:00 **Designing for the Human Element in Security**

M. Angela Sasse (University College London, UK)

12:00 – 13:30 **Lunch**

13:30 – 14:30 **Keynote: A Look at Designed-In Security Needs and Preliminary Successes**

Bill Scherlis (Carnegie Mellon University)

14:30 – 15:00 **Refreshments**

15:00 – 15:45 **Keynote: The Role of Domain-Specific Techniques in Designed-In Security**

John Launchbury (Galois, Inc.)

15:45 – 16:30 **Designed-In Security for Mobile Applications**

Jonathan Aldrich (Carnegie Mellon University)

16:30 – 17:15 **Margrave: Query-Based Policy Analysis**

Dan Dougherty (Worcester Polytechnic Institute)

17:15 **Conference Adjourned**