PROGRAM AGENDA

Tuesday, May 5

Theme: Proof Engineering

0800	Breakfast | Registration
0900	**Keynote Presentation:** **Proof Engineering: The Soft Side of Hard Proof** Gerwin Klein (NICTA)
1000	**Cerberus: Towards an Executable Semantics for Sequential and Concurrent C11** Kayvan Memarian (University of Cambridge)
1030	Refreshments
1100	**Verifiable C: Proving Functional Correctness of C Programs in Coq, e.g. SHA-256 and HMAC** Andrew Appel (Princeton University)
1130	**Deep Specifications and Certified Abstraction Layers** Ronghui Gu (Yale University)
1200	Lunch (on your own)
1330	**Qualification of Formal Methods Tools** Darren Cofer (Rockwell Collins)
1400	**Issues, Challenges, and Opportunities in the Qualification of Formal Methods Tools** Cesare Tinelli (University of Iowa)
1430	Refreshments
1500	**Multi-Language and Multi-Prover Verification with SAWScript** Aaron Tomb (Galois, Inc.)
1530	**CodeHawk: Sound Static Analysis for Proving the Absence of Memory Related Software Vulnerabilities** Douglas Smith (Kestrel Technology)
1600	**Adjourn for the Day**

PROGRAM AGENDA

Wednesday, May 6

Theme: Sustainable Integrity

0800	Breakfast | Registration
0900	**Keynote Presentation: Detecting Malice in Commodity Software** Tim Fraser (DARPA)
1000	**Remote Attestation for Cloud-Based Systems** Perry Alexander (University of Kansas)
1030	Refreshments
1100	**Software Defenses Inspired by Biodiversity** Michael Franz (University of California, Irvine)
1130	**Not-quite-so-broken TLS: Lessons in Re-engineering a Security Protocol Specification and Implementation** David Kaloper Meršinjak (University of Cambridge)
1200	Lunch (on your own)
1330	**Rigorous Architectural Modelling for Production Multiprocessors** Shaked Flur, Kathryn Gray, and Christopher Pulte (University of Cambridge)
1400	**A Formal Specification of x86 Memory Management** Shilpi Goel and Warren Hunt (UT Austin)
1430	**Language-based Hardware Verification with ReWire: Just Say No! to Semantic Archaeology** William Harrison (University of Missouri)
1500	Refreshments
1530	**Achieving High Speed and High Assurance in a Hardware-Based Cross-Domain System using Guardol** David Hardin (Rockwell Collins)
1600	**Bringing Hardware Hacking to Life** Colin O'Flynn (Dalhousie University)
1630	**Adjourn for the Day**

PROGRAM AGENDA

Thursday, May 7

Theme: Privacy

0800	Breakfast | Registration
0900	**Keynote Presentation: Building Privacy-Aware Computing Systems: An Overview of Current Capabilities and Technical Challenges** Shantanu Rane (PARC)
1000	**Reconciling Provable Security and Practical Cryptography: A Programming Language Perspective** Gilles Barth (IMDEA Software Institute)
1030	**Poster Session & Refreshments**
1115	**A Cut Principle for Information Flow** Joshua Guttman (The MITRE Corporation and WPI)
1145	**Models and Games for Quantifying Vulnerability of Secret Information** Piotr Mardziel (University of Maryland)
1215	Lunch (on your own)
1345	**NSA Civil Liberties & Privacy: Bridging the Art and Science of Privacy** Rebecca Richards (National Security Agency)
1430	**High Assurance Cryptography Synthesis with Cryptol** Joseph Kiniry (Galois, Inc.)
1500	**Poster Session & Refreshments**
1545	**Privacy through Accountability** Anupam Datta (Carnegie Mellon University)
1630	**Private Disclosure of Information** Daniel Aranki (UC Berkeley)
1700	**Conference Adjourned**