**IEEE Symposium on Computer Security Foundations, June 23-25, 2008**

| MONDAY JUNE 23 | CSF Adamson Wing Baker Hall 136A |
|---|---|
| 8:00-9:00 | **Registration & Breakfast** (Giant Eagle lobby, Baker Hall A51) |
| 9:00-9:05 | **Welcoming Remarks (**Adamson Wing) Anupam Datta, Andrei Sabelfeld |
|  | **Language-Based Security** Chair: Stephen Chong |
| 9:05-9:35 | Michele Bugliesi, Riccardo Focardi *Language Based Secure Communication* |
| 9:35-10:05 | Jesper Bengtson, Karthikeyan Bhargavan, Cedric Fournet, Andy Gordon, Sergio Maffeis *Refinement Types for Secure Implementations* |
| 10:05-10:35 | Sruthi Bandhakavi, William Winsborough, Marianne Winslett *A Trust Management Approach for Flexible Policy Management in Security-Typed Languages* |
| 10:35-11:15 | **Break** Giant Eagle lobby |
|  | **Security Models in Theory and Practice** Chair: Iliano Cervesato |
| 11:15-11:45 | Michael Clarkson, Fred Schneider *Hyperproperties* |
| 11:45-12:15 | Ann Miura-Ko, Benjamin Yolken, John Mitchell, Nicholas Bambos *Security Decision-Making Among Interdependent Organizations* |
| 12:15-2:00 | **Lunch** Giant Eagle lobby |

**IEEE Symposium on Computer Security Foundations, June 23-25, 2008**

| MONDAY JUNE 23 | CSF Adamson Wing Baker Hall 136A |
|---|---|
| | **Declassification and Erasure** Chair: Michael Backes |
| 2:00-2:30 | Gilles Barthe, Salvador Cavadini, Tamara Rezk *Tractable Enforcement of Declassification Policies* |
| 2:30-3:00 | Stephen Chong, Andrew C. Myers *End-to-end Enforcement of Erasure and Declassification* |
| 3:00-3:30 | **Break** Giant Eagle lobby |
| 3:30-5:00 | **Short Talks** (5 minutes each) Chair: Andrei Sabelfeld |
| 5:00-5:30 | **CSF Business Meeting** Chair: Jonathan Millen |
| 6:00 - | **CSF Banquet** Le Mont Restaurant Bus transportation provided |

| TUESDAY JUNE 24 | CSF/LICS Joint Session, McConomy Auditorium |
|---|---|
| 8:00 AM | **Registration & Breakfast** Rangos 2 & 3, University Center |
| 8:25 AM | **Welcome** McConomy Auditorium |
| 8:30-9:30 | **Joint CSF/LICS Invited Talk** Chairs: Frank Pfenning, Andrei Sabelfeld David Basin (joint work with Christoph Sprenger) *Cryptographically Sound Protocol-Model Abstractions* |
| | **Joint Session: Authorization Logic 1** Chairs: Andrei Sabelfeld, Frank Pfenning |
| 9:30-10:00 | Rohit Chadha, A. Prasad Sistla, Manesh Viswanathan *On the Expressiveness and Complexity of Randomization in Finite State Monitors* |
| 10:00-10:30 | Henry DeYoung, Deepak Garg, Frank Pfenning *An Authorization Logic with Explicit Time* |
| 10:30-11:00 | **Break** Rangos 2 & 3 |
| | **Joint Session: Authorization Logic 2** Chair: John Mitchell |
| 11:00-11:30 | Yuri Gurevich, Itay Neeman *DKAL: Distributed-Knowledge Authorization Language* |
| 11:30-12:00 | Glenn Bruns, Michael Huth *Access-Control Policies via Belnap Logic: Effective and Efficient Composition and Analysis* |
| 12:00-12:30 | Jeffrey Vaughan, Limin Jia, Karl Mazurak, Steve Zdancevic *Evidence-based Audit* |
| 12:30-2:00 | **Lunch** Rangos 2 & 3 |

| TUESDAY JUNE 24 | LICS Giant Eagle Auditorium Baker Hall A51 | CSF Adamson Wing Baker Hall 136A |
|---|---|---|
| | **Logical Frameworks** Chair: Robert Harper | **Protocol Analysis I** Chair: Cedric Fournet |
| 2:00-2:30 | Andrew Gacek, Dale Miller, Gopalan Nadathur *Combining Generic Judgments with Recursive Definitions* | Michael Backes, Catalin Hritcu, Matteo Maffei *Automated Verification of Remote Electronic Voting Protocols in Applied Pi-calculus* |
| 2:30-3:00 | Christian Urban, James Cheney, Stefan Berghofer *Mechanizing the Theory of LF* | Christopher Dilloway, Gavin Lowe *Specifying Secure Transport Layers* |
| 3:00-3:30 | Marcelo Fiore *Second-Order & Dependently-Sorted Abstract Syntax* | Jean Goubault-Larrecq *Towards Producing Formally Checkable Security Proofs, Automatically* |
| 3:30-4:00 | Carsten Schuermann, Jeffrey Sarnat *Structural Logical Relations* | Stephanie Delaune, Steve Kremer, Mark Ryan *Composition of Password-Based Protocols* |
| 4:00-4:30 | **BREAK** Giant Eagle Lobby | |
| | **Lambda Calculus** Chair: Ugo Dal Lago | **Cryptographic Foundations** Chair: Bruno Blanchet |
| 4:30-5:00 | Makoto Tatsuta *Types for Hereditary Permutators* | Michael Backes, Dominique Unruh *Computational Soundness of Symbolic Zero-Knowledge Proofs Against Active Attackers* |
| 5:00-5:30 | Adria Gascon, Guillem Godoy, Manfred Schmidt-Schauss *Context Matching for Compressed Terms* | Ralf Kuesters, Max Tuengerthal *Joint State Theorems for Public-Key Encryption & Digital Signature Functionalities with Local Computation* |
| 5:30-6:30 | **SHORT TALKS** Giant Eagle Auditorium Chair: Frank Pfenning | |
| 7:00-9:00 | **BREAK Giant Eagle Lobby** | |

**IEEE Symposium on Computer Security Foundations, June 23-25, 2008**

| WEDNESDAY JUNE 25 | LICS<br>Giant Eagle Auditorium | CSF<br>Adamson Wing |
|---|---|---|
| 8:30-9:30 | **LICS Invited Talk** (Giant Eagle Auditorium)<br>Chair: Stephen Brookes<br><br>Dexter Kozen<br>*Non-local Flow of Control and Kleene Algebra with Tests* | |
| | **Algebraic Methods** | **Information flow & concurrency**<br>Chair: Riccardo Focardi |
| 9:30-10:00 | Gordon Plotkin, Matija Pretnar<br>*A Logic for Algebraic Effects* | Tachio Terauchi<br>*A Type System for Observational Determinism* |
| 10:00-10:30 | Emmanuel Beffara<br>*An Algebraic Process Calculus* | Ron van der Meyden, Chenyi Zhang<br>*Information Flow in Systems with Schedulers* |
| 10:30-11:00 | **BREAK** Giant Eagle Lobby | |
| | **Process Calculi**<br>Chair: Marcelo Fiore | **Protocol Analysis II**<br>Chair: Vitaly Shmatikov |
| 11:00-11:30 | Ivan Lanese, Jorge Perez, Davide Sangiorgi, Alan Schmitt<br>*On the Expressiveness and Decidability of Higher-Order Process Calculus* | 11:15 Doug Kuhlman, Ryan Moriarty, Tony Braskich, Steve Emeott, Mahesh Tripunitara<br>*A Correctness Proof of a Mesh Security Architecture* |
| 11:30-12:00 | Taolue Chen, Wan Fokkink<br>*On the Axiomatizability of Impossible Futures: Preorder versus Equivalence* | 11:45 Stephanie Delaune, Steve Kremer, Graham Steel<br>*Formal Analysis of PKCS#11* |
| 12:00-12:30 | Sam Staton<br>*General Structural Operational Semantics through Categorical Logic* | 12:15 Closing remarks & Award presentation |
| 12:30-2:00 | **LUNCH** Rangos 2 & 3 | |