22nd IEEE Computer Security Foundations Symposium

Wednesday, 8 July 2009

8:00 – 9:00 Breakfast

9:00 – 10:30 Session on Protocol Design (Session Chair: Joshua Guttman)

- **More Anonymous Onion Routing Through Trust**
  Aaron Johnson and Paul Syverson

- **Minimal message complexity of asynchronous multi-party contract signing**
  Sjouke Mauw, Sasa Radomirovic and Mohammad Torabi Dashti

- **Authentication without Elision: Partially Specified Protocols, Associated Data, and Cryptographic Models Described by Code**
  Phillip Rogaway and Till Stegers

10:30 – 11:00 Break

11:00 – 12:00 Invited Talk by Brendan Eich, Chief Technology Officer, Mozilla Corp.
Improving JavaScript's Default Security Model with Information Flow
(Session Chair: John Mitchell)

12:00 – 14:00 Lunch

14:00 – 15:00 Session on Information Flow (Session Chair: Michael Backes)

- **Tight Enforcement of Information-Release Policies for Dynamic Languages**
  Aslan Askarov and Andrei Sabelfeld

- **Updatable Security Views**
  J. Nathan Foster, Benjamin Pierce and Steve Zdancewic

15:00 – 16:00 Session on Web Security (Session Chair: Andrew D. Gordon)

- **Language-Based Isolation of Untrusted JavaScript**
  Sergio Maffeis and Ankur Taly

- **Securing Timeout Instructions in Web Applications**
  Alejandro Russo and Andrei Sabelfeld

16:00 – 16:30 Break

16:30 – 18:00 Session on Protocol Analysis (Session Chair: Véronique Cortier)

- **Modeling and Verifying Physical Properties of Security Protocols for Wireless Networks**
  Patrick Schaller, Benedikt Schmidt, David Basin and Srdjan Capkun

- **Cryptographic Protocol Synthesis and Verification for Multiparty Sessions**
  Karthikeyan Bhargavan, Ricardo Corin, Pierre-Malo Deniélou, Cédric Fournet and James Leifer

- **A Secure Cryptographic Token Interface**
  Christian Cachin and Nishanth Chandran

19:00 – 21:00 Reception, generously supported by CA, Inc.

Thursday, 9 July 2009

8:00 – 9:00 Breakfast

9:00 – 10:30 Session on Protocols (Session Chair: Bruno Blanchet)

- **Using ProVerif to Analyze Protocols with Diffie-Hellman Exponentiation**
  Ralf Küsters and Tomasz Truderung

- **ASPIER: An Automated Framework for Verifying Security Protocol Implementations**
  Sagar Chaki and Anupam Datta

- **Inputs of Coma: Static Detection of Denial-of-Service Vulnerabilities**
  Richard Chang, Guofei Jiang, Franjo Ivančić, Sriram Sankaranarayanan and Vitaly Shmatikov

10:30 – 11:00 Break

11:00 – 12:30 Session on Authorization (Session Chair: Andrei Sabelfeld)

- **Specification and Analysis of Dynamic Authorisation Policies**
  Moritz Y. Becker

- **Policy Compliance in Collaborative Systems**
  Paul Rowe, Max Kanovich and Andre Scedrov

- **Advice from Belnap Policies**
  Flemming Nielson, Chris Hankin and Hanne Riis Nielson

12:30 – 14:00 Lunch

14:00 – 15:30 Session on Verification Methods (Session Chair: Vitaly Shmatikov)

- **Expressive power of definite clauses for verifying authenticity**
  Gilberto Filé and Roberto Vigo

- **A method for proving observational equivalence**
  Veronique Cortier and Stephanie Delaune

- **Decidable Analysis for a Class of Cryptographic Group Protocols with Unbounded Lists**
  Najah Chridi, Mathieu Turuani and Michael Rusinowitch

15:30 – 16:00 Break

16:00 – 17:15 Short Talks (Session Chair: Anupam Datta)

17:15 – 17:45 Business Meeting

19:00 – 22:00 Banquet

Friday, 10 July 2009

8:00 – 9:00 Breakfast

9:00 – 10:30 Session on Protocols (Session Chair: Jon Millen)

- **Universally Composable Symmetric Encryption**
  Ralf Küsters and Max Tuengerthal

- **Achieving Security Despite Compromise Using Zero-knowledge**
  Michael Backes, Martin Grochulla, Cătălin Hrițcu and Matteo Maffei

- **A Provably Secure And Efficient Countermeasure Against Timing Attacks**
  Boris Köpf and Markus Dürmuth

10:30 – 11:00 Break

11:00 – 12:00 Panel on Rigorous Security Analysis of Software (Moderator: Michael Backes)

Panelists: Anupam Datta, Andrew D. Gordon, Andrei Sabelfeld, David Wagner

12:00 – 2:00 Lunch