FINAL PROGRAM

2007 IEEE Symposium on Security and Privacy

May 20-23, 2007

The Claremont Resort, Berkeley/Oakland, California, USA

Sponsored by the
IEEE Computer Society Technical Committee on Security and Privacy
in co-operation with
The International Association for Cryptologic Research (IACR)

Sunday, May 20

16:00-19:00	**Registration and Reception**

Monday, May 21

7:30-9:00	Continental breakfast
9:00-9:15	**Opening Remarks** (Deborah Shands, Birgit Pfitzmann)
9:15-10:15	**Keynote Talk** *Reflections on the Future of Security and Privacy* Peter G. Neumann
10:15-10:45	Break
10:45-12:15	**Session: Network Security** Session Chair: Birgit Pfitzmann *Accurate Real-time Identification of IP Prefix Hijacking* Xin Hu and Z. Morley Mao *DSSS-Based Flow Marking Technique for Invisible Traceback* Wei Yu, Xinwen Fu, Steve Graham, Dong Xuan and Wei Zhao *On the Safety and Efficiency of Firewall Policy Deployment* Charles C. Zhang, Marianne Winslett and Carl A. Gunter
12:15-13:45	Lunch
13:45-15:30	**Session: Authentication** Session Chair: Tuomas Aura *The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies* Stuart Schechter, Rachna Dhamija, Andy Ozment and Ian Fischer

	Cryptanalysis of a Cognitive Authentication Scheme Philippe Golle and David Wagner *(15 minutes)* *A Systematic Approach to Uncover Security Flaws in GUI Logic* Shuo Chen, José Meseguer, Ralf Sasse, Helen J. Wang and Yi-Min Wang *Forward-Secure Sequential Aggregate Authentication* Di Ma and Gene Tsudik *(15 minutes)* *Extended abstract: Provable-Security Analysis of Authenticated Encryption in Kerberos* Alexandra Boldyreva and Virendra Kumar *(15 minutes)*
15:30-16:00	Break
16:00-17:30	**Session: 5-minute Work-in-Progress Talks** Session Chair: Yoshi Kohno
18:00-20:00	**Reception**

Tuesday, May 22

7:30-9:00	Continental breakfast
9:00-10:30	**Session: Privacy** Session Chair: Ninghui Li *Endorsed E-Cash* Jan Camenisch, Anna Lysyanskaya and Mira Meyerovich *Network Flow Watermarking Attack on Low-Latency Anonymous Communication Systems* Xinyuan Wang, Shiping Chen and Sushil Jajodia *Improving the Robustness of Private Information Retrieval* Ian Goldberg
10:30-11:00	Break
11:00-12:15	**Session: Access Control and Audit** Session Chair: Dan Wallach *Beyond Stack Inspection: A Unified Access-Control and Information-Flow Security Model* Marco Pistoia, Anindya Banerjee and David A. Naumann *Usable Mandatory Integrity Protection for Operating Systems* Ninghui Li, Ziqing Mao and Hong Chen *Enforcing Semantic Integrity on Untrusted Clients in Networked Virtual Environments (Extended abstract)* Somesh Jha, Stefan Katzenbeisser, Christian Schallhart, Helmut Veith and Stephen Chenney *(15 minutes)*

12:15-13:45	Lunch
13:45-15:15	**Session: Information Flow** Session Chair: Anupam Datta *Information Flow in the Peer-Reviewing Process (Extended Abstract)* Michael Backes, Markus Duermuth and Dominique Unruh *(15 minutes)* *A Cryptographic Decentralized Label Model* Jeffrey A. Vaughan and Steve Zdancewic *Gradual Release: Unifying Declassification, Encryption and Key Release Policies* Aslan Askarov and Andrei Sabelfeld *Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control* Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, Angela Schuett Reninger *(15 minutes)*
15:15-15:45	Break
15:45-17:30	**Session: Host Security** Session Chair: Crispin Cowen *Exploring Multiple Execution Paths for Malware Analysis* Andreas Moser, Christopher Kruegel and Engin Kirda *Lurking in the Shadows: Identifying Systemic Threats to Kernel Data* Arati Baliga, Pandurang Kamat and Liviu Iftode *(15 minutes)* *ShieldGen: Automatic Data Patch Generation for Unknown Vulnerabilities with Informed Probing* Weidong Cui, Marcus Peinado, Helen J. Wang and Michael Locasto *(30 minutes)* *Minimal TCB Code Execution* Jonathan M. McCune, Bryan Parno, Adrian Perrig, Michael K. Reiter and Arvind Seshadri *(15 minutes)* *Using Rescue Points to Navigate Software Recovery (Short Paper)* Stelios Sidiroglou, Oren Laadan, Angelos Keromytis and Jason Nieh *(15 minutes)*
17:30-17:45	Break
17:45-18:30	**Business Meeting**

Wednesday, May 23

7:30-9:00	Continental breakfast
9:00-10:30	**Session: Hardware and Replication** Session Chair: Wenke Lee *Moats and Drawbridges: An Isolation Primitive for Reconfigurable Hardware Based Systems* Ted Huffmire, Brett Brotherton, Gang Wang, Tim Sherwood, Ryan Kastner, Timothy Levin, Thuy Nguyen and Cynthia Irvine *Trojan Detection using IC Fingerprinting* Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi and Berk Sunar*)* *On the Optimal Communication Complexity of Multiphase Protocols for Perfect Communication* Kannan Srinathan, N. R. Prasad and C. Pandu Rangan
10:30-11:00	Break
11:00-12:30	**Session: Encryption** Session Chair: Patrick McDaniel *Ciphertext-Policy Attribute-Based Encryption* John Bethencourt, Amit Sahai and Brent Waters *Attacking the IPsec Standards in Encryption-only Configurations* Jean Paul Degabriele and Kenneth Graham Paterson *Multi-Dimensional Range Query over Encrypted Data* Elaine Shi, John Bethencourt, T.-H. Hubert Chan, Dawn Song and Adrian Perrig
12:30-12:45	**Closing Remarks** (Patrick McDaniel, Avi Rubin, and Yong Guan)
11:00-13:00	Boxed lunch