PROGRAM

2006 IEEE Symposium on Security and Privacy

May 21-24, 2006

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 21, 2006
16:00-19:00	**Registration and Reception**
	Monday, May 22, 2006
8:45-9:00	**Opening Remarks** (Hilarie Orman, Vern Paxson)
9:00-10:30	**Session: Signature Generation** (Christopher Kruegel) (30 minute talks) *Towards Automatic Generation of Vulnerability-Based Signatures* David Brumley, James Newsome, Dawn Song, Hao Wang and Somesh Jha Carnegie Mellon University, USA, and University of Wisconsin, USA *Misleading Worm Signature Generators Using Deliberate Noise Injection* Roberto Perdisci, David Dagon, Wenke Lee, Prahlad Fogla and Monirul Sharif University of Cagliari, Italy, and Georgia Institute of Technology, USA *Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience* Zhichun Li, Manan Sanghi, Yan Chen, Ming-Yang Kao and Brian Chavez Northwestern University, USA
10:30-11:00	Break
11:00-12:15	**Session: Detection** (Robert Cunningham) *Dataflow Anomaly Detection* Sandeep Bhatkar, Abhishek Chaturvedi and R. Sekar Stony Brook University, USA (30 minutes) *Towards a Framework for the Evaluation of Intrusion Detection Systems* Alvaro A. Cardenas, Karl Seamon and John S. Baras University of Maryland, USA (30 minutes) *Siren: Detecting Evasive Malware (Short Paper)* Kevin Borders, Xin Zhao and Atul Prakash University of Michigan, USA (15 minutes)
12:15-13:45	Lunch

13:45-15:45	**Session: Privacy** (Carl Landwehr) *Fundamental Limits on the Anonymity Provided by the MIX Technique* Dakshi Agrawal, Dogan Kesdogan, Vinh Pham, Dieter Rautenbach IBM T J Watson Research Center, USA, RWTH Aachen, Germany, and University of Bonn, Germany (30 minutes) *Locating Hidden Servers* Lasse Øverlier and Paul Syverson Norwegian Defence Research Establishment, Norway, Gjøvik University College, Norway and Naval Research Laboratory, USA (30 minutes) *Practical Inference Control for Data Cubes (Extended Abstract)* Yingjiu Li, Haibing Lu and Robert H. Deng Singapore Management University, Singapore (15 minutes) *Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks* Philippe Golle, Xiaofeng Wang, Markus Jakobsson and Alex Tsow Palo Alto Research Center, USA, and Indiana University, Bloomington, USA (30 minutes) *New Constructions and Practical Applications for Private Stream Searching (Extended Abstract)* John Bethencourt, Dawn Song and Brent Waters Carnegie Mellon University, USA, and SRI International, USA (15 minutes)
15:45-16:15	Break
16:15-17:45	**Session: 5-minute Work-in-Progress Talks**
18:00-20:00	**Reception and Posters**

	Tuesday, May 23, 2006
8:45-10:15	**Session: Formal Methods** (Susan Landau) (30 minute talks) *A Computationally Sound Mechanized Prover for Security Protocols* Bruno Blanchet; CNRS, École Normale Supérieure, Paris, France *A Logic for Constraint-based Security Protocol Analysis* Ricardo Corin, Ari Saptawijaya and Sandro Etalle University of Twente, The Netherlands, and University of Indonesia, Indonesia *Simulatable Security and Concurrent Composition* Dennis Hofheinz and Dominique Unruh; CWI, The Netherlands, and University of Karlsruhe, Germany
10:15-10:45	Break
10:45-12:15	**Session: Analyzing and Enforcing Policy** (Tuomas Aura) (30 minute talks) *Privacy and Contextual Integrity: Framework and Applications* Adam Barth, Anupam Datta, John C. Mitchell and Helen Nissenbaum Stanford University, USA, and New York University, USA *FIREMAN: A Toolkit for FIREwall Modeling and ANalysis* Lihua Yuan, Jianning Mai, Zhendong Su, Hao Chen, Chen-Nee Chuah and Prasant Mohapatra University of California, Davis, USA *Retrofitting Legacy Code for Authorization Policy Enforcement* Vinod Ganapathy, Trent Jaeger and Somesh Jha University of Wisconsin-Madison, USA, and Pennsylvania State University, USA
12:15-13:45	Lunch

13:45-15:30	**Session: Analyzing Code** (Doug Tygar) *Deriving an Information Flow Checker and Certifying Compiler for Java* Gilles Barthe, David A. Naumann and Tamara Rezk INRIA Sophia-Antipolis, France, and Stevens Institute of Technology, USA (30 minutes) *Automatically Generating Malicious Disks using Symbolic Execution* Junfeng Yang, Can Sar, Paul Twohey, Cristian Cadar and Dawson Engler; Stanford University, USA (30 minutes) *Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper)* Nenad Jovanovic, Christopher Kruegel and Engin Kirda; Vienna University of Technology, Austria (15 minutes) *Cobra: Fine-grained Malware Analysis using Stealth Localized-Executions* Amit Vasudevan and Ramesh Yerraballi; University of Texas Arlington, USA (30 minutes)
15:30-16:00	Break
16:00-17:15	**Session: Authentication** (Paul Van Oorschot) *Integrity (I) codes: Message Integrity Protection and Authentication Over Insecure Channels* Mario Cagalj, Srdjan Capkun, Ramkumar Rengaswamy, Ilias Tsigkogiannis, Mani Srivastava and Jean-Pierre Hubaux École Polytechnique Fédérale de Lausanne (EPFL), Switzerland, Technical University of Denmark, Denmark, and University of California, Los Angeles, USA (30 minutes) *Cognitive Authentication Schemes Safe Against Spyware (Short Paper)* Daphna Weinshall Hebrew University of Jerusalem, Israel (15 minutes) *Cache Cookies for Browser Authentication (Extended Abstract)* Ari Juels, Markus Jakobsson and Tom N. Jagatic RSA Laboratories, USA, RavenWhite Inc., USA, and Indiana University, USA (15 minutes) *Secure Device Pairing based on a Visual Channel (Short Paper)* Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen and N. Asokan University of California, Irvine, USA, and Nokia Research Center, Finland (15 minutes)
17:15-17:30	Break
17:30-18:30	**Business Meeting**

	Wednesday, May 24, 2006
9:00-10:15	**Session: Attacks** (Kevin Fu) *SubVirt: Implementing malware with virtual machines* Samuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski, Helen J. Wang, Jacob R. Lorch University of Michigan, USA, and Microsoft Research, USA (30 minutes) *Practical Attacks on Proximity Identification Systems (Short Paper)* Gerhard P. Hancke University of Cambridge, UK (15 minutes) *On the Secrecy of Timing-Based Active Watermarking Trace-Back Techniques* Pai Peng, Peng Ning and Douglas S. Reeves North Carolina State University, USA (30 minutes)
10:15-10:45	Break
10:45-12:30	**Session: Systems** (Helen Wang) *A Safety-Oriented Platform for Web Applications* Richard S. Cox, Jacob Gorm Hansen, Steven D. Gribble, and Henry M. Levy University of Washington, USA, and University of Copenhagen, Denmark (30 minutes) *Tamper-Evident, History-Independent, Subliminal-Free Data Structures on PROM Storage -or- How to Store Ballots on a Voting Machine (Extended Abstract)* David Molnar, Tadayoshi Kohno, Naveen Sastry and David Wagner University of California, Berkeley, USA, and University of California, San Diego, USA (15 minutes) *Analysis of the Linux Random Number Generator* Zvi Gutterman, Benny Pinkas and Tzachy Reinman Hebrew University, Israel, Haifa University, Israel, and Safend, Israel (30 minutes) *The Final Nail in WEP's Coffin* Andrea Bittau, Mark Handley and Joshua Lackey University College London, UK, and Microsoft, USA (30 minutes)