PRELIMINARY PROGRAM

2003 IEEE Symposium on Security and Privacy

May 11-14, 2003
The Claremont Resort
Oakland, California, USA

sponsored by
IEEE Computer Society Technical Committee on Security and Privacy
in cooperation with
The International Association for Cryptologic Research (IACR)

Sunday, May 11, 2003

4:00-7:00	Registration and Reception

Monday, May 12, 2003

8:45-9:00	Opening Remarks
9:00-10:30	**Session: Anonymity** *Mixminion: Design of a Type III Anonymous Remailer Protocol* George Danezis (Cambridge Univ.), Roger Dingledine, Nick Mathewson (Free Haven Project) *Probabilistic Treatment of MIXes to Hamper Traffic Analysis* Dakshi Agrawal (IBM Watson), Dogan Kesdogan, Stefan Penz (Aachen Univ. Tech.) *Defending Anonymous Communication Against Passive Logging Attacks* Matt Wright, Micah Adler, Brian Neil Levine, Clay Shields (U. Mass.)
10:30-11:00	Break
11:00-12:00	**Session: IDS** *Active Mapping: Resisting NIDS Evasion Without Altering Traffic* Umesh Shankar (UC Berkeley), Vern Paxson (ICSI) *Anomaly Detection Using Call Stack Information* Henry Hanping Feng (U. Mass.), Oleg M. Kolesnikov, Prahlad Fogla, Wenke Lee (Georgia Tech.), Weibo Gong (U. Mass.)
12:00-1:30	Lunch
1:30-2:30	**Invited talk**
2:30-3:00	Break
3:00-4:00	**Session: OS** *Defending Against Denial-of-Service Attacks with Puzzle Auctions* XiaoFeng Wang, Mike Reiter (CMU) *Pi: A Path Identification Mechanism to Defend against DDoS Attacks* Abraham Yaar, Adrian Perrig, Dawn Song (CMU)
4:00-6:00	5-minute talks

Tuesday, May 13, 2003

9:00-10:30	**Session: Formal Methods** *A Unified Scheme for Resource Protection in Automated Trust Negotiation* Ting Yu, Marianne Winslett (U. Illinois, Urbana-Champaign) *Beyond Proof-of-compliance: Safety and Availability Analysis in Trust Management* Ninghui Li (Stanford), William H. Winsborough (NAI Labs), John C. Mitchell (Stanford) *Intransitive Non-Interference for Cryptographic Purposes* Michael Backes, Birgit Pfitzmann (IBM Zurich)
10:30-11:00	Break
11:00-12:00	**Session: Hardware** *Specifying and Verifying Hardware for Tamper-Resistant Software* David Lie, John Mitchell (Stanford), Chandramohan Thekkath (Microsoft Research), Mark Horowitz (Stanford) *Using Memory Errors to Attack a Virtual Machine* Sudhakar Govindavajhala, Andrew W. Appel, (Princeton)
12:00-1:30	Lunch
1:30-2:30	**Invited talk**
2:30-3:00	Break
3:00-4:00	**Session: Hardware & Crypto** *Secret Handshakes from Pairing-Based Key Agreements* D. Balfanz, G. Durfee (PARC), N. Shankar (U. Maryland), D.K. Smetters, J. Staddon, H.C. Wong (PARC) *Random Key Predistribution Schemes for Sensor Networks* Haowen Chan, Adrian Perrig, Dawn Song (CMU)

Wednesday, May 14, 2003

9:00-10:30	**Session: Distributed Systems** *Hardening Functions for Large Scale Distributed Computations* Douglas Szajda, Barry Lawson, Jason Owen (U. Richmond) *A Practical Revocation Scheme for Broadcast Encryption Using Smart Cards* Noam Kogan, Yuval Shavitt, Avishai Wool (Tel Aviv Univ.) *Using Replication and Partitioning to Build Secure Distributed Systems* Lantian Zheng, Stephen Chong, Andrew C. Myers (Cornell), Steve Zdancewic (U. Pennsylvania)
10:30-11:00	Break
11:00-12:00	*Vulnerabilities in Synchronous IPC Designs* Jonathan S. Shapiro (Johns Hopkins) *Garbage Collector Memory Accounting in Language-Based Systems* David W. Price, Algis Rudys, Dan S. Wallach (Rice)