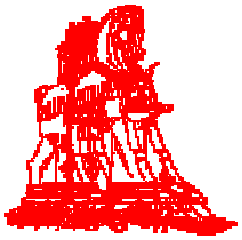

ADVANCE PROGRAM

May 13-16,2001
The Claremont Resort
Oakland, California, USA

2001 IEEE Symposium on Security and Privacy

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

Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for the presentation of developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field.

General chair:	Li Gong (Sun Microsystems, USA) (li.gong@sun.com)
Vice chair:	Heather Hinton (Tivoli Systems, USA) (hhinton@tivoli.com)
Program co-chairs:	Roger Needham (Microsoft Research, UK) (needham@microsoft.com)
	Martin Abadi (InterTrust, USA) (abadi@cs.stanford.edu)
Treasurer:	Brian Loe (Secure Computing Corporation, USA)

Advance Registration until April 9, 2001
Hotel Rooms held for Symposium until April 13, 2001 (5pm, Pacific Standard Time)
Registration and Hotel Information available from www.ieee-security.org/TC/sp2001.html

Advanced Program

Sunday, 13 May 2001

4:00- 7:00 Registration and Reception

Monday, 14 May 2001

8:45-9:00 Opening remarks

9:00-10:30 *Session: Tamper-resistance and Cryptography*
Cryptographic Security for Mobile Code
Joy Algesheimer, Christian Cachin, Jan Camenisch, Günter Karjoth (IBM Research)
Networked Cryptographic Devices Resilient to Capture
Philip MacKenzie, Michael Reiter (Bell Labs, Lucent)
Protection of Keys against Modification Attack
Wai-wa Fung, Mordecai Golin, Jim Gray, (Hong Kong UST)

10:30-11:00 Break

11:00-12:00 *Session: Intrusion and anomaly detection, I*
Data Mining Methods for Detection of New Malicious Executables
Matthew Schultz, Eleazar Eskin, Erez Zadok, Sal Stolfo (Columbia University)
Evaluation of Intrusion Detectors: A Decision Theory Approach
John Gaffney (Lockheed Martin), Jacob Ulvila (Decision Science Associates, Inc)

12:00- 1:30 Lunch

1:30- 2:30 *Session: Information flow*
On Confidentiality and Algorithms
Johan Agat, David Sands (Chalmers University of Technology)
Preserving Information Flow Properties under Refinement
Heiko Mantel (German Research Centre for Artificial Intelligence, DFKI)

2:30- 3:00 Break

3:00- 4:30 *Session: Access control and trust management*
Understanding Trust Management Systems
Stephen Weeks (InterTrust Technologies)
SD3: a trust management system with certified evaluation
Trevor Jim (AT&T Labs Research)
Formal Treatment of Certificate Revocation Under Communal Access Control
Xuhui Ao, Naftaly Minsky, Victoria Ungureanu (Rutgers University)

Tuesday, 15 May 2001

9:00-10:30 *Session: Intrusion and Anomaly Detection II*
Information-Theoretic Measures for Anomaly Detection
Wenke Lee, Dong Xiang (North Carolina State University)
A Fast Automaton-Based Method for Detecting Anomalous Program Behaviors
R Sekar (SUNY), Mugdha Bendre (SUNY at Stony Brook), Pradeep Bollineni
Intrusion Detection via Static Analysis
David Wagner (UC Berkeley), Drew Dean (Xerox PARC)

10:30-11:00 Break

11:00-12:00 *Session: Cryptographic Protocols, I*
Performance of Public Key-Enabled Kerberos Authentication in Large Networks
Alan Harbitter (PEC Solutions), Daniel A. Menasce (George Mason University)
A Model for Asynchronous Reactive Systems and its Application to Secure Message Transmission
Birgit Pfitzmann (Universitat des Saarlandes), Michael Waidner (IBM Research)

12:00- 1:30 Lunch

1:30- 2:30 *Session: What's really different*
Cryptographic Key Generation from Voice
Fabian Monrose, Michael Reiter, Qi Li, Susanne Wetzel (Bell Labs, Lucent)
A Trend Analysis of Exploitations
Hilary Browne, William Arbaugh (UM-CP), John McHugh, William Fithen (CERT/CC)

2:30- 3:00 Break

3:00- 5:00 *5-minute presentations on developing research*

5:00- 5:45 Security and Privacy Technical Committee Meeting

Wednesday, 16 May 2001

9:00-10:30 *Invited Talk:* **Reverse Engineering: A Legal Right or Wrong?**
Speaker: Pamela Samuelson
School of Information Management and Systems, University of California at Berkeley

10:30-11:00 Break

11:00-12:00 *Session: Cryptographic protocols, 2*
Graph-Based Authentication of Digital Streams
Sara Miner (UC San Diego), Jessica Staddon
ELK, a New Protocol for Efficient Large-Group Key Distribution
Adrian Perrig, Dawn Song, J. D. Tygar (UC Berkeley)