

Proceedings

2003

**Symposium on
Security and Privacy**

Proceedings

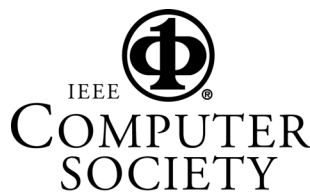
2003

Symposium on

Security and Privacy

May 11 – 14, Berkeley, California, USA

Sponsored by
IEEE Computer Society Technical Committee on Security and Privacy



<http://computer.org>

Los Alamitos, California

Washington • Brussels • Tokyo

Copyright © 2003 by The Institute of Electrical and
Electronics Engineers, Inc.
All rights reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number PR01940
ISBN 0-7695-1940-7
ISSN Number 1081-6011

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1-714-821-8380
Fax: + 1-714-821-4641
E-mail: cs.books@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1-732-981-0060
Fax: + 1-732-981-9667
[http://shop.ieee.org/store/
customer-service@ieee.org](http://shop.ieee.org/store/customer-service@ieee.org)

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81-3-3408-3118
Fax: + 81-3-3408-3553
tokyo.ofc@computer.org

Editorial production by Bob Werner
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House


COMPUTER
SOCIETY

 **IEEE**

Table of Contents

2003 IEEE Symposium on Security and Privacy

Message from the Program Chairs	vii
Program Committee.....	viii

Session: Anonymity

Mixminion: Design of a Type III Anonymous Remailer Protocol	2
<i>G. Danezis, R. Dingledine, and N. Mathewson</i>	
Probabilistic Treatment of MIXes to Hamper Traffic Analysis	16
<i>D. Agrawal, D. Kesdogan, and S. Penz</i>	
Defending Anonymous Communications Against Passive Logging Attacks	28
<i>M. Wright, M. Adler, B. Levine, and C. Shields</i>	

Session: IDS

Active Mapping: Resisting NIDS Evasion without Altering Traffic.....	44
<i>U. Shankar and V. Paxson</i>	
Anomaly Detection Using Call Stack Information	62
<i>H. Feng, O. Kolesnikov, P. Fogla, W. Lee, and W. Gong</i>	

Session: OS

Defending Against Denial-of-Service Attacks with Puzzle Auctions	78
<i>X. Wang and M. Reiter</i>	
Pi: A Path Identification Mechanism to Defend against DDoS Attacks.....	93
<i>A. Yaar, A. Perrig, and D. Song</i>	

Session: Formal Methods

A Unified Scheme for Resource Protection in Automated Trust Negotiation.....	110
<i>T. Yu and M. Winslett</i>	
Beyond Proof-of-Compliance: Safety and Availability Analysis in Trust Management.....	123
<i>N. Li, W. Winsborough, and J. Mitchell</i>	
Intransitive Non-Interference for Cryptographic Purposes.....	140
<i>M. Backes and B. Pfitzmann</i>	

Session: Hardware

Using Memory Errors to Attack a Virtual Machine	154
<i>S. Govindavajhala and A. Appel</i>	
Specifying and Verifying Hardware for Tamper-Resistant Software	166
<i>D. Lie, J. Mitchell, C. Thekkath, and M. Horowitz</i>	

Session: Hardware & Crypto

Secret Handshakes from Pairing-Based Key Agreements	180
<i>D. Balfanz, G. Durfee, N. Shankar, D. Smetters, J. Staddon, and H. Wong</i>	
Random Key Predistribution Schemes for Sensor Networks	197
<i>H. Chan, A. Perrig, and D. Song</i>	

Session: Distributed Systems

Hardening Functions for Large Scale Distributed Computations	216
<i>D. Szajda, B. Lawson, and J. Owen</i>	
A Practical Revocation Scheme for Broadcast Encryption Using Smart Cards	225
<i>N. Kogan, Y. Shavitt, and A. Wool</i>	
Using Replication and Partitioning to Build Secure Distributed Systems	236
<i>L. Zheng, S. Chong, A. Myers, and S. Zdancewic</i>	
Vulnerabilities in Synchronous IPC Designs	251
<i>J. Shapiro</i>	
Garbage Collector Memory Accounting in Language-Based Systems	263
<i>D. Price, A. Rudys, and D. Wallach</i>	

Author Index	275
---------------------------	------------