

Proceedings

# 1997 IEEE Symposium on Security and Privacy

May 4-7, 1997  
Oakland, California

***Sponsored by***

IEEE Computer Society Technical Committee  
on Security and Privacy

***In cooperation with***

International Association of Cryptologic Research (IACR)



IEEE Computer Society Press  
Los Alamitos, California

Washington • Brussels • Tokyo

---

HTC EX. 1027



---

IEEE Computer Society Press  
10662 Los Vaqueros Circle  
P.O.Box 3014  
Los Alamitos, CA 90720-1264

---

Copyright © 1997 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 1331, 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 Press, or the Institute of Electrical and Electronics Engineers, Inc.*

---

IEEE Catalog Number 97CB36097  
ISBN 0-8186-7828-3 (softbound)  
ISBN 0-7803-4159-7 (casebound)  
ISBN 0-8186-7830-5 (microfiche)  
ISSN: 1081-6011

*Additional copies may be ordered from:*

IEEE Computer Society Press  
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  
Email: [cs.books@computer.org](mailto:cs.books@computer.org)

IEEE Service Center  
445 Hoes Lane  
P.O. Box 1331  
Piscataway, NJ 08855-1331  
Tel: +1-908-981-1393  
Fax: +1-908-981-9667  
[misc.custserv@computer.org](mailto:misc.custserv@computer.org)

IEEE Computer Society  
13, Avenue de l'Aquilon  
B-1200 Brussels  
BELGIUM  
Tel: +32-2-770-2198  
Fax: +32-2-770-8505  
[euro.ofc@computr.org](mailto:euro.ofc@computr.org)

IEEE Computer Society  
Ooshima Building  
2-19-1 Minami-Aoyama  
Minato-ku, Tokyo 107  
JAPAN  
Tel: +81-3-3408-3118  
Fax: +81-3-3408-3553  
[tokyo.ofc@computer.org](mailto:tokyo.ofc@computer.org)

Editorial production by Penny Storms  
Cover by Joseph Daigle / Studio Productions  
Printed in the United States of America by The Printing House



The Institute of Electrical and Electronics Engineers, Inc.

# Table of Contents

## 1997 IEEE SYMPOSIUM ON SECURITY AND PRIVACY

Message from the Program Chairs .....	viii
Conference Committee .....	ix

### Panel/Debate

<i>Moderator:</i>	<i>John D. McLean, Naval Research Laboratory</i>	
<i>Arguing in favor:</i>	<i>Lead: Bob Blakley, IBM</i>	
	<i>Second: Darrell Kienzle, University of Virginia</i>	
<i>Opposed:</i>	<i>Lead: William R. Shockley, Consultant</i>	
	<i>Second: James P. Downey, Naval Postgraduate School</i>	
Is the Trusted Computing Base Concept Fundamentally Flawed?.....		2
	<i>J. McLean</i>	
Some Weaknesses of the TCB Model.....		3
	<i>B. Blakley and D.M. Kienzle</i>	
Is the Reference Monitor Concept Fatally Flawed? The Case for the Negative.....		6
	<i>W.R. Shockley and J.P. Downey</i>	

### Authorization and Authentication

Toward Acceptable Metrics of Authentication.....		10
	<i>M.K. Reiter and S.G. Stubblebine</i>	
An Authorization Scheme for Distributed Object Systems.....		21
	<i>V. Nicomette and Y. Deswarte</i>	
A Logical Language for Expressing Authorizations.....		31
	<i>S. Jajodia, P. Samarati, and V.S. Subrahmanian</i>	

### Applications

Anonymous Connections and Onion Routing .....		44
	<i>P.F. Syverson, D.M. Goldschlag, and M.G. Reed</i>	
The Design and Implementation of a Multilevel Secure Log Manager .....		55
	<i>V.R. Pesati, T.F. Keefe, and S. Pal</i>	
A Secure and Reliable Bootstrap Architecture .....		65
	<i>A. Arbaugh, D.J. Farber, and J.M. Smith</i>	
An MBone Proxy for an Application Gateway Firewall.....		72
	<i>K. Djahandari and D. Sterne</i>	

### Security Theory

Secure Software Architectures .....		84
	<i>M. Moriconi, X. Qian, R.A. Riemenschneider, and L. Gong</i>	
A General Theory of Security Properties .....		94
	<i>A. Zakinthinos and E.S. Lee</i>	
Analyzing Consistency of Security Policies.....		103
	<i>L. Cholvy and F. Cuppens</i>	

**Panel: Ensuring Assurance in Mobile Computing**

*Moderator: Marvin Schaefer, Arca Systems*  
*Panel Members: Sylvan Pinsky, National Security Agency*  
*Drew Dean, Princeton University*  
*Li Gong, JavaSoft*  
*Jim Roskind, Netscape*  
*Barbara Fox, Microsoft*

Ensuring Assurance in Mobile Computing ..... 114  
*M. Schaefer, S. Pinsky, D. Dean, L. Gong, J. Roskind, and B. Fox*

**Architectures**

Filtering Postures: Local Enforcement for Global Policies ..... 120  
*J.D. Guttman*  
Providing Flexibility in Information Flow Control for Object-Oriented Systems ..... 130  
*E. Ferrari, P. Samarati, E. Bertino, and S. Jajodia*  
Automated Analysis of Cryptographic Protocols Using Murø ..... 141  
*J.C. Mitchell, M. Mitchell, and U. Stern*

**Intrusion Detection and Beyond**

How to Systematically Classify Computer Security Intrusions ..... 154  
*U. Lindqvist and E. Jonsson*  
Surviving Information Warfare Attacks on Databases ..... 164  
*P. Ammann, S. Jajodia, C.D. McCollum, and B.T. Blaustein*  
Execution Monitoring of Security-Critical Programs in a Distributed  
Systems: A Specification-Based Approach ..... 175  
*C. Ko, M. Ruschitzka, and K. Levitt*  
Catalytic Inference Analysis: Detecting Inference Threats due to Knowledge  
Discovery ..... 188  
*J. Hale and S. Shenoi*

**Panel: Security in Innovative New Operating Systems**

*Moderator: Cynthia E. Irvine, Naval Postgraduate School*  
*Panel Members: Brian Bershad, University of Washington (Spin Project)*  
*Frans Kaashoek, MIT (Exokernel Project)*  
*Jay Lepreau, University of Utah (Flux Project)*  
*George Necula, Carnegie Mellon University (Fox Project)*  
*Larry Peterson, University of Arizona (Scout Project)*

Security in Innovative New Operating Systems ..... 202  
*C.E. Irvine*  
Research on Proof-Carrying Code for Untrusted-Code Security ..... 204  
*G. Necula and P. Lee*  
Access Control for the SPIN Extensible Operating System ..... 205  
*R. Grimm and B.N. Bershad*  
Escort: Securing Scout Paths ..... 206  
*O. Spatscheck and L. Peterson*

## System Vulnerabilities

Analysis of a Denial of Service Attack on TCP .....	208
<i>C.L. Schuba, I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram, and D. Zamboni</i>	
Deniable Password Snatching: On the Possibility of Evasive Electronic Espionage .....	224
<i>A. Young and M. Yung</i>	
Number Theoretic Attacks on Secure Password Schemes .....	236
<i>S. Patel</i>	
<b>Author Index</b> .....	249