
FOUNDATIONS OF INTRUSION TOLERANT SYSTEMS

Edited by

Jaynarayan H. Lala
OASIS Program Manager, 1999-2003



**Organically Assured and
Survivable Information Systems**
OASIS



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 reflect the authors' opinions. 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 PR02057
ISBN 0-7695-2057-X
Library of Congress Number 2003113550

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: + 1 800 272 6657
Fax: + 1 714 821 4641
<http://computer.org/cspress>
csbooks@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

Individual paper REPRINTS may be ordered at: reprints@computer.org

Editorial production by Stephanie Kawada

Cover art production by Joe Daigle/Studio Productions

Printed in the United States of America by Victor Graphics, Inc.



OASIS

**Foundations of
Intrusion Tolerant Systems**
Edited by Jaynarayan H. Lala



ORGANICALLY ASSURED AND SURVIVABLE INFORMATION SYSTEMS

Foundations of Intrusion Tolerant Systems



Published by the IEEE Computer Society Press
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314

IEEE Computer Society Press Order Number PR02057
Library of Congress Number 2003113550
ISBN 0-7695-2057-X



Table of Contents

Preface	viii
Introduction	x
Bibliography	426

Intrusion Tolerant Databases

Architectures for Intrusion Tolerant Database Systems	3
<i>P. Liu</i>	
The Design of an Adaptive Intrusion Tolerant Database System	14
<i>P. Luenam and P. Liu</i>	

Proof-Carrying Code

Foundational Proof-Carrying Code	25
<i>A. W. Appel</i>	
Type-Preserving Compilation of Featherweight Java.....	35
<i>C. League, Z. Shao, and V. Trifonov</i>	
A Type System for Certified Binaries	60
<i>Z. Shao, V. Trifonov, B. Saha, and N. Papaspyrou</i>	

Certification Authorities

Protecting Privacy Using the Decentralized Label Model.....	89
<i>A. C. Myers and B. Liskov</i>	
Enforceable Security Policies	117
<i>F. B. Schneider</i>	
Untrusted Hosts and Confidentiality: Secure Program Partitioning	138
<i>S. Zdancewic, L. Zheng, N. Nystrom, and A. C. Myers</i>	
COCA: A Secure Distributed Online Certification Authority	152
<i>L. Zhou, F. B. Schneider, and R. van Renesse</i>	

Intrusion Tolerant Storage

Self-Securing Storage: Protecting Data in Compromised Systems	195
<i>J. D. Strunk, G. R. Goodson, M. L. Scheinholtz, C. A. N. Soules, and G. R. Ganger</i>	

Linux Security

Linux Security Modules: General Security Support for the Linux Kernel	213
<i>C. Wright, C. Cowan, S. Smalley, J. Morris, and G. Kroah-Hartman</i>	
Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade.....	227
<i>C. Cowan, P. Wagle, C. Pu, S. Beattie, and J. Walpole</i>	

Group Communications

Quantifying the Cost of Providing Intrusion Tolerance in Group Communication Systems.....	241
<i>H. V. Ramasamy, P. Pandey, J. Lyons, M. Cukier, and W. H. Sanders</i>	
Formal Specification and Verification of a Group Membership Protocol for an Intrusion-Tolerant Group Communication System	251
<i>H. V. Ramasamy, M. Cukier, and W. H. Sanders</i>	
Survival by Defense-Enabling	261
<i>P. Pal, F. Webber, and R. Schantz</i>	

System Reconfiguration

Protection of Software-Based Survivability Mechanisms	273
<i>C. Wang, J. Davidson, J. Hill, and J. Knight</i>	
Design and Evaluation of a Wide-Area Event Notification Service.....	283
<i>A. Carzaniga, D. S. Rosenblum, and A. L. Wolf</i>	

Mobile-Code Security

Making Mobile Code Both Safe and Efficient	337
<i>M. Franz, W. Amme, M. Beers, N. Dalton, P. H. Fröhlich, V. Haldar, A. Hartmann, P. S. Housel, F. Reig, J. von Ronne, C. H. Stork, and S. Zhenochin</i>	

Intrusion Tolerant Servers

SITAR: A Scalable Intrusion-Tolerant Architecture for Distributed Services	359
<i>F. Wang, F. Jou, F. Gong, C. Sargor, K. Goseva-Popstojanova, and K. Trivedi</i>	

The Design and Implementation of an Intrusion Tolerant System	368
<i>J. Reynolds, J. Just, E. Lawson, L. Clough, R. Maglich, and K. Levitt</i>	
Learning Unknown Attacks—A Start.....	374
<i>J. E. Just, J. C. Reynolds, L. A. Clough, M. Danforth, K. N. Levitt, R. Maglich, and J. Rowe</i>	
Developing a Heterogeneous Intrusion Tolerant CORBA System.....	387
<i>D. Sames, B. Matt, B. Niebuhr, G. Tally, B. Whitmore, and D. Bakken</i>	
Wrappers	
Hardening COTS Software with Generic Software Wrappers	399
<i>T. Fraser, L. Badger, and M. Feldman</i>	
Detecting and Countering System Intrusions Using Software Wrappers	414
<i>C. Ko, T. Fraser, L. Badger, and D. Kilpatrick</i>	
Author Index	435