Security and Privacy 1996

Proceedings

1996 IEEE Symposium on Security and Privacy

May 6 – 8, 1996

Oakland, California

Sponsored by the

IEEE Computer Society Technical Committee on Security and Privacy

In cooperation with the

International Association of Cryptologic Research (IACR)

IEEE Computer Society Press
Los Alamitos, California

Washington • Brussels • Tokyo

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

Copyright © 1996 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 96CB35924
ISBN 0-8186-7417-3 (softbound)
ISBN 0-7803-3227-0 (casebound)
ISBN 0-7803-3228-7 (microfiche)
ISSN 1081-4011

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

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: +1-908-981-1393
Fax: +1-908-981-9667
mis.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@computer.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

Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by KNI, Inc.

The Institute of Electrical and Electronics Engineers, Inc.

Table of Contents

1996 IEEE Symposium on Security and Privacy

Message from the Program Chairs ____ vii

Conference Committee ____ viii

Covert Channels

An Analysis of the Timed Z-Channel ____ 2
Ira S. Moskowitz, Steven J. Greenwald, Myong H. Kang

Defining Noninterference in the Temporal Logic of Actions ____ 12
Todd Fine

Panel: Goals for Computer Security Education

Panelists: Cynthia Irvine, Chair, Leslie Chalmers, Karl Levitt, Stephen F. Barnett
Jim Schindler, Roger R. Schell

Goals for Computer Security Education ____ 24
Cynthia E. Irvine

Computer Security Training and Education: A Needs Analysis ____ 26
Stephen F. Barnett

Domain Specific Security

A Security Policy Model for Clinical Information Systems ____ 30
Ross Anderson

Protocols

What do We Mean by Entity Authentication? ____ 46
Dieter Gollmann

A Fair Non-repudiation Protocol ____ 55
Jianying Zhou, Dieter Gollmann

Limitations on Design Principles for Public Key Protocols ____ 62
Paul Syverson

Databases

Ensuring Atomicity of Multilevel Transactions ____ 74
Paul Ammann, Sushil Jajodia, Indrakshi Ray

View-Based Access Control with High Assurance ____ 85
Xiaolei Qian

Supporting Multiple Access Control Policies in Database Systems 94
Elisa Bertino, Sushil Jajodia, Pierangela Samarati

Biologically Inspired Topics in Computer Security

An Immunological Approach to Change Detection:
Algorithms, Analysis, and Implications 110
Patrik D'haeseleer, Stephanie Forrest, Paul Helman

A Sense of Self for UNIX Processes 120
Stephanie Forrest, Steven A. Hofmeyr,
Anil Somayaji, Thomas A. Longstaff

Cryptovirology: Extortion-Based Security Threats and Countermeasures 129
Adam Young, Moti Yung

Modeling

A Security Model of Dynamic Labeling Providing a Tiered Approach to Verification 142
Simon Foley, Li Gong, Xiaolei Qian

A Communication Agreement Framework for Access/Action Control 154
Martin Röscheisen, Terry Winograd

Decentralized Trust Management 164
Matt Blaze, Joan Feigenbaum, Jack Lacy

Security Properties and CSP 174
Steve Schneider

Networks

Java Security: From HotJava to Netscape and Beyond 190
Drew Dean, Edward W. Felten, Dan S. Wallach

On Two Proposals for On-line Bankcard Payments using Open Networks:
Problems and Solutions 201
Wenbo Mao

Secure Network Objects 211
Leendert van Doorn, Martín Abadi,
Mike Burrows, Edward Wobber

Run-Time Security Evaluation (RTSE) for Distributed Applications 222
Cristina Serban, Bruce McMillin

Index of Authors 233