

PROCEEDINGS

13TH ANNUAL  
COMPUTER SECURITY  
APPLICATIONS CONFERENCE

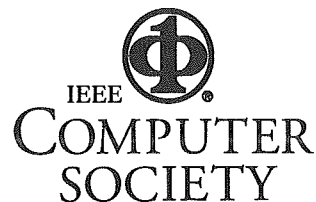
San Diego, California  
December 8-12, 1997

*Sponsored by*

Applied Computer Security Associates

in cooperation with

ACM Special Interest Group on Security, Audit, and Control



Los Alamitos, California

Washington • Brussels • Tokyo

QA76.9  
.A25C65  
1997

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 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 PR08274  
ISBN 0-8186-8274-4  
ISBN 0-8186-8275-2 (case)  
ISBN 0-8186-8276-0 (microfiche)  
IEEE Order Plan Catalog Number 97TB100213  
ISSN 1063-9527

*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: + 1-908-981-1393  
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

Editorial production by Bookmark Media

Cover art production by Joe Daigle/Studio Productions

Printed in the United States of America by Technical Communication Services

IEEE   
COMPUTER  
SOCIETY



3-27-98 602

# TABLE OF CONTENTS

## 13th Annual Computer Security Applications Conference—ACSAC'97

Conference Committee .....	ix
Program Committee .....	x
Tutorial Committee .....	x
Reviewers .....	x

### TRACK A, WEDNESDAY, DECEMBER 10

#### VIRTUAL MONEY

SESSION CHAIR: K. Keus

Micro-Digital Money for Electronic Commerce .....	2
<i>K. Nguyen, Y. Mu, V. Varadharajan</i>	
Secure and Efficient Digital Coins .....	9
<i>K. Nguyen, Y. Mu, V. Varadharajan</i>	
The Secure Distribution of Digital Contents .....	16
<i>E. von Faber, R. Hammelrath, F. Heider</i>	

#### ASSURANCE

SESSION CHAIR: J. Adams

Simple Assured Bastion Hosts .....	24
<i>C. Cant, S. Wiseman</i>	
Kernel and Shell-Based Applications Integrity Assurance .....	34
<i>G. Mohay, J. Zellers</i>	
Risk Assessment for Large Heterogeneous Systems .....	44
<i>J. Freeman, T. Darr, R. Neely</i>	

<b>PANEL: PRODUCT ASSURANCE</b> .....	54
---------------------------------------	----

MODERATOR: J. Adams

Panelists: D. Gambel, E. Weiss, M. Aldrich

## TRACK B, WEDNESDAY, DECEMBER 10

### FORUM: EVOLVING THE EVALUATION PARADIGM .....56

MODERATOR: M. Schanken

Speakers: K. Britton, G. Copeland

### DATABASE SECURITY

SESSION CHAIR: L. Notargiacomo

Securing an Object Relational Database .....59  
*S. Lewis, S. Wiseman*

Supporting Secure Canonical Upgrade Policies in Multilevel Secure Object Stores .....69  
*S. Foley*

Incremental Assurance for Multilevel Applications .....81  
*D. Thompson, M. Denz*

### NETWORK SECURITY

SESSION CHAIR: S. LaFountain

An Efficient Message Authentication Scheme for Link State Routing .....90  
*S. Cheung*

Detection and Classification of TCP/IP Network Services .....99  
*K. Tan, B. Collie*

Achieving User Privacy in Mobile Networks .....108  
*B. Askwith, M. Merabti, Q. Shi, K. Whiteley*

## TRACK A, THURSDAY, DECEMBER 11

### PLENARY PANEL SESSION: CRITICAL INFRASTRUCTURE PROTECTION— THE CYBER/INFORMATION DIMENSION: REPORT ON NATIONAL INFRASTRUCTURE COORDINATION INITIATIVES .....118

MODERATOR: S. League

Panelists: D. Keyes, D. Knauf, M. Woods

### GUARDS AND FIREWALLS

SESSION CHAIR: E. Siarkiewicz

Domain and Type Enforcement Firewalls .....122  
*K. Oostendorp, L. Badger, C. Vance, W. Morrison, D. Sherman, D. Sterne*

A Reference Model for Firewall Technology .....133  
*C. Schuba, E. Spafford*

Using Type Enforcement to Assure a Configurable Guard .....146  
*P. Greve, J. Hoffman, R. Smith*

**FORUM: ASSURANCE LESSONS LEARNED** .....155  
MODERATOR: J. Adams

Speakers: B. Dawson, D. Baker, T. Filsinger, K. Ferraiolo, R. Hefner

**ACCESS CONTROL**

SESSION CHAIR: E. Coyne

Implementing RBAC on a Type Enforced System .....158  
*J. Hoffman*

Lattice Based Models for Controlled Sharing of Confidential Information in the  
Saudi Hajj System .....164  
*T. Himdi, R. Sandhu*

Using Kernel Hypervisors to Secure Applications .....175  
*T. Mitchem, R. Lu, R. O'Brian*

**TRACK B, THURSDAY, DECEMBER 11**

**SECURITY ARCHITECTURE**

SESSION CHAIR: J. Heaney

Applying the DoD Goal Security Architecture as a Methodology for the  
Development of System and Enterprise Security Architectures .....183  
*T. Lowman, D. Mosier*

An Architecture for Multilevel Secure Interoperability .....194  
*M. Kang, J. Froscher, I. Moskowitz*

Using Web Technologies in Two MLS Environments:A Security Analysis .....205  
*R. Niemeyer*

**CRYPTOGRAPHY AND KEY MANAGEMENT**

SESSION CHAIR: M. Bishop

On the Key Recovery of the Key Escrow System .....216  
*Y. Lee, C. Liah*

Threshold and Generalized DSS Signatures without a Trusted Party .....221  
*C. Wang, T. Hwang*

An Improved E-Mail Security Protocol .....227  
*B. Schneier, C. Hall*

**FORUM: PKI**

MODERATOR: A. Friedman

Speakers: T. Burke, P. Mellinger, B. Thompson, G. Moore

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.