

Proceedings



Fourth IEEE International Workshop on Information Assurance

IWIA 2006

13-14 April 2006 • Royal Holloway, United Kingdom

Editors

John L. Cole
Stephen D. Wolthusen



Los Alamitos, California

Washington • Tokyo

Copyright © 2006 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 P2564
ISBN-13: 978-0-7695-2564-8
ISBN-10: 0-7695-2564-4
Library of Congress Number 2006921087

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 Documation LLC



IEEE Computer Society
Conference Publishing Services

<http://www.computer.org/proceedings/>

Proceedings



Fourth IEEE International Workshop on Information Assurance

IWIA 2006

Table of Contents

Message from the Workshop Chairs	vii
Program Committee	viii

Session I: Intrusion Detection and Prevention I

The LAIDS/LIDS Framework for Systematic IPS Design.....	3
<i>Simon P. Chung and Aloysius K. Mok</i>	
An Intelligent Detection and Response Strategy to False Positives and Network Attacks.....	12
<i>Emmanuel Hooper</i>	
Active Event Correlation in Bro IDS to Detect Multi-stage Attacks.....	32
<i>Bing Chen, Joohan Lee, and Annie S. Wu</i>	

Session II: Evaluation and Criteria

Designing a Secure Point-of-Sale System	51
<i>Allan Pedersen, Anders Hedegaard, and Robin Sharp</i>	
High Robustness Requirements in a Common Criteria Protection Profile	66
<i>Thuy D. Nguyen, Timothy E. Levin, and Cynthia E. Irvine</i>	

Session III: Modeling and Engineering Software Security

Ensuring Compliance between Policies, Requirements and Software Design: A Case Study	79
<i>Qingfeng He, Paul Otto, Annie I. Antón, and Laurie Jones</i>	
A Remote IT Security Evaluation Scheme: A Proactive Approach to Risk Management	93
<i>Suleyman Kondakci</i>	

Session IV: Defending Communication Systems

Present and Future Challenges concerning DoS-Attacks against PSAPs in VoIP Networks	103
<i>Nils Aschenbruck, Matthias Frank, Peter Martini, Jens Tölle, Roland Legat, and Heinz-Dieter Richmann</i>	
Jamming Commercial Satellite Communications during Wartime: An Empirical Study	109
<i>Hank Rausch</i>	

Session V: Intrusion Detection and Prevention II

An Application of Information Theory to Intrusion Detection	119
<i>E. Earl Eiland and Lorie M. Liebrock</i>	
HonIDS: Enhancing Honeypot System with Intrusion Detection Models	135
<i>Yong Tang, HuaPing Hu, XiCheng Lu, and Jie Wang</i>	
POSEIDON: A 2-Tier Anomaly-Based Network Intrusion Detection System	144
<i>Damiano Bolzoni, Sandro Etalle, Pieter Hartel, and Emmanuele Zambon</i>	

Session VI: Modeling Security

Modeling and Execution of Complex Attack Scenarios Using Interval Timed Colored Petri Nets	157
<i>Ole Martin Dahl and Stephen D. Wolthusen</i>	
Factoring High Level Information Flow Specifications into Low Level Access Controls	169
<i>Kevin Kahley, Manigandan Radhakrishnan, and Jon A. Solworth</i>	

Author Index	187
---------------------------	-----