

---

## **INTEGRITY AND INTERNAL CONTROL IN INFORMATION SYSTEMS VI**

## **IFIP – The International Federation for Information Processing**

IFIP was founded in 1960 under the auspices of UNESCO, following the First World Computer Congress held in Paris the previous year. An umbrella organization for societies working in information processing, IFIP's aim is two-fold: to support information processing within its member countries and to encourage technology transfer to developing nations. As its mission statement clearly states,

*IFIP's mission is to be the leading, truly international, apolitical organization which encourages and assists in the development, exploitation and application of information technology for the benefit of all people.*

IFIP is a non-profitmaking organization, run almost solely by 2500 volunteers. It operates through a number of technical committees, which organize events and publications. IFIP's events range from an international congress to local seminars, but the most important are:

- The IFIP World Computer Congress, held every second year;
- Open conferences;
- Working conferences.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is small and by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is less rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

Any national society whose primary activity is in information may apply to become a full member of IFIP, although full membership is restricted to one society per country. Full members are entitled to vote at the annual General Assembly, National societies preferring a less committed involvement may apply for associate or corresponding membership. Associate members enjoy the same benefits as full members, but without voting rights. Corresponding members are not represented in IFIP bodies. Affiliated membership is open to non-national societies, and individual and honorary membership schemes are also offered.

# INTEGRITY AND INTERNAL CONTROL IN INFORMATION SYSTEMS VI

*IFIP TC11 / WG11.5 Sixth Working Conference on  
Integrity and Internal Control in Information Systems (IICIS)  
13–14 November 2003, Lausanne, Switzerland*

*Edited by*

**Sushil Jajodia**

*George Mason University  
Fairfax, Virginia, USA*

**Leon Strous**

*De Nederlandsche Bank NV  
Amsterdam, The Netherlands*

**KLUWER ACADEMIC PUBLISHERS**

NEW YORK, BOSTON, DORDRECHT, LONDON, MOSCOW

eBook ISBN: 1-4020-7901-X  
Print ISBN: 1-4020-7900-1

©2004 Kluwer Academic Publishers  
New York, Boston, Dordrecht, London, Moscow

Print ©2004 Kluwer Academic Publishers  
Boston

All rights reserved

No part of this eBook may be reproduced or transmitted in any form or by any means, electronic, mechanical, recording, or otherwise, without written consent from the Publisher

Created in the United States of America

Visit Kluwer Online at: <http://kluweronline.com>  
and Kluwer's eBookstore at: <http://ebooks.kluweronline.com>

# CONTENTS

---

Preface	vii
Acknowledgements	ix
<b>Part one. Refereed papers</b>	
1. <i>Remote Integrity Checking</i> Yves Deswarte, Jean-Jacques Quisquater, Ayda Saïdane	1
2. <i>Automated Checking of SAP Security Permissions</i> Sebastian Höhn, Jan Jürjens	13
3. <i>A Formal Analysis of a Digital Signature Architecture</i> David Basin, Kunihiro Miyazaki, Kazuo Takaragi	31
4. <i>Using Parameterized UML to Specify and Compose Access Control Models</i> Indrakshi Ray, Na Li, Dae-Kyoo Kim, Robert France	49
5. <i>Enforcing Integrity in Multimedia Surveillance</i> Naren B. Kodali, Csilla Farkas, Duminda Wijesekera	67
6. <i>A Learning-based Approach to Information Release Control</i> Claudio Bettini, X. Sean Wang, Sushil Jajodia	83
7. <i>Information Security Governance using ISO 17799 and COBIT</i> Elmari Pretorius, Basie von Solms	107
8. <i>Tracing Attacks and Restoring Integrity with LASCAR</i> Alexandre Aellig, Philippe Oechslin	115
9. <i>A Secure Multi-sited Version Control System</i> Indrajit Ray, Junxing Zhang	125
10. <i>Integration of Integrity Constraints in Database Federations</i> Herman Balsters, Bert de Brock	143
11. <i>Reducing Disruption in Time-Table Condition Monitoring</i> Binling Jin, Suzanne M. Embury	159

12. <i>A Service Oriented System Based Information Flow Model for Damage Assessment</i> Yanjun Zuo, Brajendra Panda	177
13. <i>An Efficient OODB Model for Ensuring the Integrity of User-defined Constraints</i> Belal Zaqibeh, Hamidah Ibrahim, Ali Mamat, Md. Nasir Sulaiman	195
<b>Part two. Invited papers</b>	
14. <i>From Security Culture to Effective E-security Solutions</i> Solange Ghernaouti-Hélie	209
15. <i>Consistent Query Answering: Recent Developments and Future Directions</i> Jan Chomicki	219
16. <i>Role of Certification in Meeting Organisation Security Requirements</i> William List	241
<b>Part three. Panel session</b>	
17. <i>Grand Challenges in Data Integrity and Quality</i> Bhavani Thuraisingham	249
Index of contributors	255
Index of keywords	257

# PREFACE

---

The development and integration of integrity and internal control mechanisms into information system infrastructures is a challenge for researchers, IT personnel and auditors. Since its beginning in 1997, the IICIS international working conference has focused on the following questions:

- what precisely do business managers need in order to have confidence in the integrity of their information systems and their data and what are the challenges IT industry is facing in ensuring this integrity;
- what are the status and directions of research and development in the area of integrity and internal control;
- where are the gaps between business needs on the one hand and research / development on the other; what needs to be done to bridge these gaps.

This sixth volume of IICIS papers, like the previous ones, contains interesting and valuable contributions to finding the answers to the above questions. We want to recommend this book to security specialists, IT auditors and researchers who want to learn more about the business concerns related to integrity. Those same security specialists, IT auditors and researchers will also value this book for the papers presenting research into new techniques and methods for obtaining the desired level of integrity.

It is the hope of all who contributed to IICIS 2003 that these proceedings will inspire readers to join the organizers for the next conference on integrity and internal control in information systems. You are invited to take the opportunity to contribute to next year's debate with colleagues and submit a paper or attend the working conference. Check the websites given below regularly for the latest information.

We thank all those who have helped to develop these proceedings and the conference. First of all, we thank all the authors who submitted papers as well as the keynote and invited speakers, and those who presented papers and participated in the panel. Finally, we would like to thank all conference participants, IFIP and the sponsors and supporters of this conference.

January 2004

Sushil Jajodia  
Leon Strous

## Websites:

IFIP TC-11 Working group 11.5 IICIS 2004  
<http://www.cs.colostate.edu/~iicis04/>

IFIP TC-11 Working group 11.5  
[http://csis.gmu.edu/faculty/Tc11\\_5.html](http://csis.gmu.edu/faculty/Tc11_5.html)

IFIP TC-11  
<http://www.ifip.tu-graz.ac.at/TC11>

IFIP  
<http://www.ifip.org>

## Still available:

- IICIS 2002: Integrity and internal control in information systems V  
ed. Michael Gertz  
ISBN 1-4020-7473-5
- IICIS 2001: Integrity, internal control and security in information systems:  
Connecting governance and technology  
ed. Michael Gertz, Erik Guldentops, Leon Strous  
ISBN 1-4020-7005-5
- IICIS 1999: Integrity and internal control in information systems: Strategic  
views on the need for control  
ed. Margaret E. van Biene-Hershey, Leon Strous  
ISBN 0-7923-7821-0
- IICIS 1998: Integrity and internal control in information systems  
ed. Sushil Jajodia, William List, Graeme McGregor, Leon Strous  
ISBN 0-412-84770-1
- IICIS 1997: Integrity and internal control in information systems: Volume 1,  
Increasing the confidence in information systems  
ed. Sushil Jajodia, William List, Graeme McGregor, Leon Strous  
ISBN 0-412-82600-3



# ACKNOWLEDGEMENTS

---

## **Conference chairs:**

Stefano Spaccapietra, Swiss Federal Institute of Techn., Lausanne, CH  
Serge Vaudenay, Swiss Federal Institute of Technology, Lausanne, CH

## **Programme Committee:**

### *Co-Chairs:*

Sushil Jajodia, George Mason University, USA  
Leon Strous, De Nederlandsche Bank, The Netherlands

### *Members/reviewers:*

David Basin, ETH Zürich, Switzerland  
Sabrina de Capitani di Vimercati, University of Milan, Italy  
Michael Gertz, University of California at Davis, USA  
Erik Guldentops, University of Antwerp, Belgium  
Klaus Kursawe, IBM, Switzerland  
Detlef Kraus, SRC, Germany  
William List, William List & Co., UK  
Refik Molva, Eurecom, France  
David Naccache, GEMPLUS, France  
Philippe Oechslin, EPF Lausanne, Switzerland  
Indrakshi Ray, Colorado State University, USA  
Arnie Rosenthal, The MITRE Corporation, USA  
Adrian Spalka, University of Bonn, Germany  
Bhavani Thuraisingham, NSF, USA

## **Organizing Committee**

Christelle Vangenot (chair)  
Marlyse Taric (secretariat)  
Swiss Federal Institute of Technology, Lausanne, Switzerland