INFORMATION SECURITY FOR
GLOBAL INFORMATION INFRASTRUCTURES
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.
INFORMATION SECURITY FOR GLOBAL INFORMATION INFRASTRUCTURES

IFIP TC11
Sixteenth Annual Working Conference on Information Security
August 22—24, 2000, Beijing, China

Edited by

Sihan Qing
Engineering Research Center for Information Security Technology
Chinese Academy of Sciences
China

Jan H.P. Eloff
Rand Afrikaans University
South Africa

SPRINGER SCIENCE+BUSINESS MEDIA, LLC
Library of Congress Cataloging-in-Publication Data


Includes bibliographical references and index.
DOI 10.1007/978-0-387-35515-3
1. Computer security—Congresses. 2. Data protection—Congresses. I. Qing, Sihan. II. Eloff, Jan H.P.

QA76.9.A25 I463 2000
005.8—dc21 00-055102

Copyright © 2000 by IFIP International Federation for Information Processing

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, mechanical, photo-copying, recording, or otherwise, without the prior written permission of the publisher, Springer Science+Business Media, LLC.

Printed on acid-free paper.
The original version of the book frontmatter was revised: The copyright line was incorrect. The Erratum to the book frontmatter is available at DOI: 10.1007/978-0-387-35515-3_53
# CONTENTS

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Author(s)</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td></td>
<td>xiii</td>
<td></td>
</tr>
<tr>
<td>Acknowledgements</td>
<td></td>
<td>xv</td>
<td></td>
</tr>
<tr>
<td>Part one - Reviewed papers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>IT Security Certification and Criteria</td>
<td>KAI RANNENBERG</td>
<td>1</td>
</tr>
<tr>
<td>4.</td>
<td>From Trusted Information Security Controls to a Trusted Information Security Environment</td>
<td>ROSSOUW VON SOLMS, HELEN VAN DE HAAR</td>
<td>29</td>
</tr>
<tr>
<td>5.</td>
<td>A Qualitative Approach to Information Availability</td>
<td>THEODORE TRYFONAS, DIMITRIS GRITZALIS, SPYROS KOKOLAKIS</td>
<td>37</td>
</tr>
<tr>
<td>7.</td>
<td>Information Security Management through Measurement</td>
<td>ELMARIE VON SOLMS, BASIE VON SOLMS</td>
<td>59</td>
</tr>
<tr>
<td>Chapter</td>
<td>Title</td>
<td>Pages</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
<td>-------</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Independent Policy Oriented Layering of Security Services</td>
<td>89</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HERBERT LEITOLD, PETER LIPP, ANDREAS STERBENZ</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Reducing Computer Fraud through Situational Crime Prevention</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ROBERT WILLISON</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MIKKO T. SIPONEN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BUKS LOUWRENS, BASIE VON SOLMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Using Smart Cards in an Educational Environment: Services and Security Features</td>
<td>131</td>
<td></td>
</tr>
<tr>
<td></td>
<td>COSTAS LAMBRINOUDAKIS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>MASS: Model for an Auditing Security System</td>
<td>141</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALIDA LIEBENBERG, JAN ELOFF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Classifying Information for External Release</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td></td>
<td>S. DAWSON, S. DE CAPITANI DI VIMERCATI, P. LINCOLN, P. SAMARATI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Using Mobile Agent Results to Create Hard-To-Detect Computer Viruses</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td></td>
<td>YONGGE WANG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>CARDS: A Distributed System for Detecting Coordinated Attacks</td>
<td>171</td>
<td></td>
</tr>
<tr>
<td></td>
<td>JIAHAI YANG, PENG NING, X.SEAN WANG, SUSHIL AJODIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Robust Audio Watermarking based on Secure Spread Spectrum and Auditory Perception Model</td>
<td>181</td>
<td></td>
</tr>
<tr>
<td></td>
<td>PETAR HORVATIC, JIAN ZHAO, NIELS J. THORWIRTH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>A Simple and Efficient Approach to Verifying Cryptographic Protocols</td>
<td>191</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SUN YONGXING, WANG XINMEI</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
21. Power Analysis of RC6 and Serpent
   Wu Wenling, Feng Dengguo, Qing Sihan

22. A Simple Algorithm for Computing Several Sequences
    Synthesis
   Wang Mingsheng, Qi Sihan, Feng Dengguo

23. GSFS – A New Group-Aware Cryptographic File System
    Claudia Eckert, Florian Erhard, Johannes Geiger

24. Robustness-Agile Encryptor for ATM Networks
    H. Leitold, W. Mayerwieser, U. Payer, K. Posch, R. Posch, J. Wolkesterforfer

25. Fast Construction of Secure Discrete Logarithm Problems
    over Jacobian Varieties
   Jinhui Chao, Kazuto Matsuo, Shigeo Tsuji

26. A New Serial/Parallel Architecture for a Low Power
    Modular Multiplier
   Johann Grobschadl

27. Defending Against Null Calls Stream Attacks by Using a
    Double-Threshold Dynamic Filter
   Haizhi Xu, Changwei Cui, Ying Lin, Tiejian Luo, Zhanqiu Dong

28. A Multi-party Non-repudiation Protocol
    Steve Kremer, Olivier Markowitch

    Jiang Shaoquan, Feng Dengguo, Qing Sihan

30. Integrated Multi-Agent Approach to Network Security
    Assurance: Models of Agents' Community
   V. Gorodetski, I. Kotenko, V. Skormin

31. Towards Network Denial of Service Resistant Protocols
    Jussipekka Leiwo, Tuomas Aura, Pekka Nikander
   ELTON SAUL, ANDREW HUTCHISON

33. Anonymous Electronic Voting System with Non-Transferable Voting Passes
   ROSANNA CHAN, JONATHAN WONG, ALEX CHAN

34. Improving Packet Filters Management through Automatic and Dynamic Schemes
   OLIVIER PAUL, MARYLINE LAURENT

35. A Context-Sensitive Access Control Model and Prototype Implementation
   DAMIAN CHOLEWKA, REINHARDT BOTHA, JAN ELOFF

36. Regulating Access to Semistructured Information on the Web
   E. DAMIANI, S. DE CAPITANI DI VIMERCATI, S. PARABOSCHI, P. SAMARATI

37. On the Practical Feasibility of Secure Distributed Computing: A Case Study
   GREGORY NEVEN, FRANK PIESSENS, BART DE DECKER

38. Elements of A Language for Role-Based Access Control
   M. HITCHENS, V. VARADHARAJAN

39. Disallowing Unauthorized State Changes of Distributed Shared Objects
   J. LEIWO, C. HÄNLE, P. HOMBURG, A. TANENBAUM

40. Framework for Security Analysis and Access Control in a Distributed Service Medical Imaging Network
   IAN GREENSHIELDS, ZHIHONG YANG

   MIKKO SIPONEN

42. Information Warfare: Fact or Fiction?
   MATTHEW WARREN, W. HUTCHINSON
43. Enforcing Privacy by Withholding Private Information 421
FRANS LATEGAN, MARTIN OLIVIER

44. The Changing Roles of Patent and Copyright Protection 431
for Software and Communication Technology in the Internet Age
GREGORY KIRSCH, TIM XIA

45. A Framework for Electronic Commerce Security 441
LES LABUSCHAGNE

46. Electronic Payment Systems with Fair On-line Verification 451
FENG BAO, ROBERT DENG, JIANYING ZHOU

47. Fair Electronic Cash Systems with Multiple Banks 461
FANGGUO ZHANG, FUTAI ZHANG, YUMIN WANG

48. Securing Mobile Agents for Electronic Commerce: an Experiment 471
A. CHAN, K. WONG, T. WONG, M. LYU

49. A Flexible Management Framework for Certificate Status Validation 481
A. CORRADI, R. MONTANARI, C. STEFANELLI, D. BERBECARU,
A. LIOY, F. MAINO

50. A Security Architecture for Electronic Commerce Applications 491
B. DE WIN, J. VAN DEN BERGH, F. MATTHIJS, B. DE DECKER,
W. JOOSEN

Part Two - Invited papers

51. On the Development of the Advanced Encryption Standard 503
YIQUN LISA YIN

52. Public Key Infrastructure: Managing the e-Business Security 505
XUEJIA LAI
Erratum to: Information Security for Global Information Infrastructures
SIHAN QING, JAN H.P. ELOFF

Index of contributors 507
PREFACE

IFIP/SEC2000, being part of the 16th IFIP World Computer Congress (WCC2000), is being held in Beijing, China from August 21 to 25, 2000. SEC2000 is the annual conference of TC11 (Information Security) of the International Federation of Information Processing. The conference focuses on the seamless integration of information security services as an integral part of the Global Information Infrastructure in the new millennium.

SEC2000 is sponsored by the China Computer Federation (CCF), IFIP/TC11, and Engineering Research Centre for Information Security Technology, Chinese Academy of Sciences (ERCIST, CAS).

There were 180 papers submitted for inclusion, 50 papers among them have been accepted as long papers and included in this proceeding, 81 papers have been accepted as short papers and published in another proceeding. All papers presented in this conference were reviewed blindly by a minimum of two international reviewers. The authors' affiliations of the 180 submissions and the accepted 131 papers range over 26 and 25 countries or regions, respectively. We would like to appreciate all who have submitted papers to IFIP/SEC2000, and the authors of accepted papers for their on-time preparation of camera-ready final versions. Without their contribution there would be no conference.

We wish to express our gratitude to all program committee members and other reviewers for their hard work in reviewing the papers in a short time and for contributing to the conference in different ways. We would like to thank Hein Venter for his time and expertise in compiling the final version of the proceedings.

Finally, we wish to take this opportunity to thank all the participants, organizers and contributors to IFIP/SEC2000.

August, 2000

Sihan Qing
Qsihan@yahoo.com
Jan Eloff
eloff@rkw.rau.ac.za
ACKNOWLEDGEMENTS

Organised by:

IFIP TC-11
China Computer Federation (CCF)
Engineering Research Center for Information Security Technology
Chinese Academy of Sciences (ERCIST, CAS)

Conference General Chair

Prof. Tang Zesheng (China)
Prof. Wang Jiesheng (China)
Prof. Basie von Solms (South Africa)

Programme Committee Chair

Prof. Qing Sihan (China)
Prof. Jan Eloff (South-Africa)

Programme Committee

Prof Sihan Qing (co-chairman), PRC
Prof Jan Eloff (co-chairman), South Africa
Prof William Caelli, Australia
Prof Pierangela Samarati, Italy
Prof Dimitris Gritzalis, Greece
Prof Hartmut Pohl, Germany
Prof Kurt Bauknecht, Switzerland
Prof Louise Yngstrom, Sweden
Prof Stephanie Teufel, Switzerland
Mr William List, UK
Dr. Gyorgy Papp, Hungary
Prof Reinhard Posch, Austria
Prof Basie von Solms, South Africa
Prof Richard Baskerville, USA
Reviewers

Baskerville, Richard, USA
Bauknecht, Kurt, Switzerland
Beatson, John, New Zealand
Berson, Thomas, USA
Botha, Reinhard, South Africa
Booysen, Hettie, South Africa
Drevin, Lynette, South Africa
Eloff, Jan, South Africa
Eloff, Mariki, South Africa
Feng, Dengguo, China
Gritzalis, Dimitris, Greece
Hutchison, Andrew, South Africa
Irvine, Cynthia, USA
Katsikas, Sokratis, Greece
Labuschagne, Les, South Africa
Lai, Xuejia, Switzerland
List, William, UK
Longley, Dennis, Australia
Lourens, Buks, South Africa
Oppliger, Rolf, Switzerland
Overbeek, Paul, The Netherlands
Papp, Gyorgy, Hungary
Pei, Dingyi, China
Pohl, Hartmut, Germany
Posch, Reinhart, Austria
Rannenberg, Kai, UK
Samarati, Pierangela, Italy
Smith, Elme, South Africa
Strous, Leon, The Netherlands
Verschuren, Jan, The Netherlands
Von Solms, Basie, South Africa
Von Solms, Rossouw, South Africa
Xiao, Guozheng, China
Yngstrom, Louise, Sweden
Yin, Lisa Yiqun, USA