SECURITY AND PRIVACY
IN THE AGE OF UNCERTAINTY
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.
SECURITY AND PRIVACY IN THE AGE OF UNCERTAINTY

IFIP TC11 18th International Conference on Information Security (SEC2003)
May 26–28, 2003, Athens, Greece

Edited by

Dimitris Gritzalis
Athens University of Economics and Business
Greece

Sabrina De Capitani di Vimercati
University of Milan
Italy

Pierangela Samarati
University of Milan
Italy

Sokratis Katsikas
University of the Aegean
Greece

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

A C.I.P. Catalogue record for this book is available from the Library of Congress.

Security and Privacy in the Age of Uncertainty
Edited by Dimitris Gritzalis, Sabrina De Capitani di Vimercati, Pierangela Samarati, and Sokratis Katsikas
DOI 10.1007/978-0-387-35691-4

Copyright © 2003 by IFIP International Federation for Information Processing

All rights reserved. No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, microfilming, recording, or otherwise, without written permission from the Publisher Springer-Science+Business Media, B.V.,
with the exception of any material supplied specifically for the purpose of being entered and executed on a computer system, for exclusive use by the purchaser of the work.

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: 10.1007/978-0-387-35691-4_52
Contents

Preface ........................................................................................................... xiii
IFIP/Sec’03 Conference Committees ........................................................... xv
IFIP/Sec’03 Workshop Program Committees .............................................. xix

PART ONE Secure Networks and Distributed Systems
Trust Mediation for Distributed Information Systems .............................. 1
Brian Toone, Michael Gertz, Premkumar Devanbu
Concerning Enterprise Network Vulnerability to HTTP Tunneling ........... 13
Constantine Daicos, Scott Knight
Providing Voice Privacy Over Public Switched Telephone Networks ...... 25
Mohamed Sharif, Duminda Wijesekera
A Multi-Party Non-Repudiation Protocol for Exchange of Different
Messages ....................................................................................................... 37
Jose Antonio Onieva, Jianying Zhou, Mildrey Carbonell,
Javier Lopez
Establishing Chain of Evidence as a Base for Non-Repudiation
Services ....................................................................................................... 49
Jing-Jang Hwang, Min-Hua Shao, Soushan Wu

PART TWO Content Protection
Securing XML-based Multimedia Content .............................................. 61
Ernesto Damiani, Sabrina De Capitani di Vimercati
Secure Audit Logging with Tamper-Resistant Hardware ......................... 73
Cheun Ngen Chong, Zhonghong Peng, Pieter H. Hartel
PCMHoDC .................................................................................................. 85
HeeJae Park, Jong Kim

PART THREE Secure Multicast Communication and
Secure Mobile Networks
Using Keystroke Analysis as a Mechanism for Subscriber
Authentication on Mobile Handsets ......................................................... 97
N.L. Clarke, Steven M. Furnell, Benn M. Lines, Paul L. Reynolds
Introducing PKI to Enhance Security in Future Mobile Networks

Georgios Kambourakis, Angelos Rouskas, Stefanos Gritzalis

A Time Driven Methodology for Key Dimensioning in Multicast Communications

Roberto Di Pietro, Luigi V. Mancini, Alessandro Mei

A Flexible Category-Based Collusion-Resistant Key Management Scheme for Multicast

Claudio Duma, Nahid Shahmehri, Patrick Lamrix

PART FOUR Security Management

Content, Context, Process Analysis of IS Security Policy Formation

Maria Karyda, Spyros Kokolakis, Evangelos Kiountouzis

Integrating Security into Systems Development

Ulrika Evertsson, Urban Örthberg, Louise Yngström

Integrating Information Security into Corporate Governance

Kerry-Lynn Thomson, Rossouw von Solms

Building an Enterprise IT Security Management System

Meletis A. Belsis, Leonid Smalov

Information Security Management System: Processes and Products

Mariki M. Eloff, Jan H.P. Eloff

PART FIVE Intrusion Prevention and Detection

Detecting Malicious Use with Unlabelled Data Using Clustering and Outlier Analysis

Scott Knight, Luciano Carosielli

E²xB: A Domain-Specific String Matching Algorithm for Intrusion Detection

Kostas G. Anagnostakis, Spyros Antonatos, P. Markatos, Michalis Polychronakis

Intrusion Masking for Distributed Atomic Operations

Meng Yu, Peng Liu, Wanyu Zang

Using Fuzzy System to Manage False Alarms in Intrusion Detection

Mehdi Shajari, Ali A. Ghorbani

An Experiment in Software Decoy Design

J. Bret Michael, Georgios Fragkos, Mikhail Auguston
PART SIX Access Control Policies and Models
A User Friendly Guard with Mobile Post-Release Access Control Policy ............................................................... 265
Douglas E. Williams, Amgad Fayad, Sushil Jajodia, Daniel Calle
Security Model for Health Care Computing and Communication Systems ........................................................................... 277
Anas Abou El Kalam, Yves Deswarte
Constrained Role-based Delegation .................................................................................................................. 289
Longhua Zhang, Gail-Joon Ahn

PART SEVEN Secure Information Systems
CSAP - An Adaptable Security Module for the E-Government System Webocrat ......................................................... 301
Fredj Dridi, Michael Fischer, Günther Pernul
Perceptions of Security Contributing to the Implementation of Secure IS ........................................................................ 313
Theodore Tryfonas, Evangelos Kiountouzis
New Directions on IS Security Methods ........................................................................................................ 325
Mikko T. Siponen
Secure Vickrey Auctions without a Trusted Third Party .................................................................................. 337
Bart De Decker, Gregory Neven, Frank Piessens

PART EIGHT Security Protocols
Integrating Logics and Process Calculi for Cryptographic Protocol Analysis ................................................................. 349
Mauricio Papa, Oliver Bremer, John Hale, Sujeet Shenoi
Flexible Delegation Security for Improved Distribution in Ubiquitous Environments ................................................. 361
Georgios Kalogridis, Chan Yeob Yeun, Gary Clemo
Cooperative Defense Firewall Protocol ........................................................................................................ 373
Magdi M.S. El-Soudani, Mohamed A. Eissa
How to turn a PIN into an Iron Beam ........................................................................................................ 385
Stefan Lucks, Ruediger Weis

PART NINE Workshop on Information Security Management
World Framework for Security Benchmark Changes .......................................................................................... 397
Lech J. Janczewski, Andrew M. Colarik
Information Security: Auditing the Behaviour of the Employee ........................................................................... 401
Cheryl Vroom, Rossouw von Solms
Priorities in the Deployment of Network Intrusion Detection Systems .......................................................... 405
*Marcin Dobrucki, Teemupekka Virtanen*

Bridging the Gap between Risk Analysis and Security Policies .......... 409
*Paul Gaunard, Eric Dubois*

Framework and Architecture for Secure Mobile Business Applications ........................................................................ 413
*Jochen Haller, Philip Robinson, Thomas Walter, Roger Kilian-Kehr*

ISO 17799 and Australian Healthcare Organisations ......................... 417
*W.J. Brooks, Mattew J. Warren, William Hutchinson*

**PART TEN Workshop on Privacy and Anonymity in Network & Distributed Systems**

Statistical Disclosure Attacks ................................................................. 421
*George Danezis*

On the Anonymity of Timed Pool Mixes .............................................. 427
*Andrei Serjantov, Richard E. Newman*

Privacy in Content Distribution Networks ........................................... 435
*R.J. Hulsebosch*

**PART ELEVEN Workshop on Small Systems Security**

Security, Fault-Tolerance and their Verification for Ambient Systems ........................................................................ 441
*Jaap-Henk Hoepman*

Hidden Layer Authentication using Smart Card for WEP-based WLANS ........................................................................ 447
*Giannis Pikrammenos, Ghassan Sarkis, John Soldatos, Vasilios Anagnostopoulos*

PINPAS: A Tool for Power Analysis of Smartcards ............................. 453
*Jerry den Hartog, Jan Vershuren, Erik de Vink, Jaap de Vos, W. Wiersma*

Assessing Security in Energy-Efficient Sensor Networks ........................ 459
*Yee Wei Law, Sandro Etalle, Pieter H. Hartel*

From Finite State Machines to Provably Correct Java Card Applets ........ 465
*Engelbert Hubbers, Martijn Oostdijk, Erik Poll*

Security Characteristics of E-Collaboration Environments .................. 471
*Bob Hulsebosch, Ernst-Jan Goedvolk, Wil Janssen*

Roadmap for Securing Handheld Devices .......................................... 477
*Preetida Vinayakray-Jani*
PART TWELVE Workshop on Security and Control of IT in Society

Lawful Cyber Decoy Policy .................................................. 483
*James Bret Michael, Thomas C. Wingfield*

Electronic Signature as a part of Information Society Infrastructure .............................................. 489
*Juhani Paavilainen, Suzana Stojakovic-Celustka, Dagmar Brechlerova*

Erratum to: Security and Privacy in the Age of Uncertainty ............ E1
*Dimitris Gritzalis, Sabrina De Capitani di Vimercati, Pierangela Samarati, Sokratis Katsikas*
Preface

This volume contains the papers selected for presentation at the 18th IFIP International Information Security Conference (IFIP/SEC-2003) and at the associated Workshops. The Conference and Workshops were held on 26-28 May 2003, in Athens, Greece, and hosted by the Athens Chamber of Commerce and Industry.

In response to the call for papers, 121 papers were submitted to the main conference track. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the Programme Committee. The Program Committee meeting was held electronically. Of the papers submitted, 33 were selected for presentation at the conference (an acceptance rate of 27%). This volume contains also 18 short papers selected with a similar process by the Workshop Committees from additional papers submitted to their Workshops.

An event like this just does not happen; it depends on the volunteering efforts of a lot of individuals, as well as on the support of the local co-organizers and of the sponsoring institutions. There is a long list of people who volunteered their time and energy to put together the conference and workshops and who deserve special thanks. We thank Bart De Decker, Simone Fisher-Hübner, Kai Rannenberg, Jan Verschuren and Matt Warren, for chairing the Workshop committees. We also thank all the members of the program committees, and the external reviewers for their hard work in the paper evaluation and Sabrina De Capitani di Vimercati who collated this volume. We are grateful to the local co-organizing institutions (the Athens Chamber of Commerce and Industry, the Athens University of Economics and Business, and the University of the Aegean) as well as to the main sponsors of the Conference (Citibank, and Ernst & Young). We are also grateful to the people whose hard work ensured a smooth organization process. Among them we would like to mention Nickolas Kyrloglou, Maria Karyda, Dimitris Lekkas, Sia Vagena.
Last, but certainly not least, our thanks go to the members of TC-11 of IFIP, who gave us the opportunity to organize this event, to all the authors who submitted papers, and to all the attendees. We hope you find the programme stimulating.

Dimitris Gritzalis, Athens University of Economics and Business
(General Chair)

Pierangela Samarati, Università di Milano
Sokratis Katsikas, University of the Aegean
(Program Chairs)
IFIP/Sec’03 Conference Committees

Conference Chairs
General Chairs: Dimitris Gritzalis, Athens University of Economics and Business (AUEB), Greece
Program Chairs: Pierangela Samarati, University of Milan, Italy
Sokratis Katsikas, University of Aegean, Greece

Program Committee
Gail-Joon Ahn, The University of North Carolina at Charlotte, USA
Helen Armstrong, Curtin University, Australia
Vijay Atluri, Rutgers University, USA
Walter Caelli, Queensland University of Technology, Australia
Sabrina De Capitani di Vimercati, University of Milan, Italy
Bart De Decker, Katholieke Universiteit Leuven, Belgium
Yves Deswarte, LAAS-CNRS, France
Michel Dupuy, SGDN/DCSSI/CERTA, France
Mahmoud T. El-Hadidi, Cairo University, Egypt
Jan Eloff, Rand Afrikaans University, South Africa
Csilla Farkas, University of South Carolina, USA
Steven Furnell, University of Plymouth, UK
Stefanos Gritzalis, University of the Aegean, Greece
Sushil Jajodia, George Mason University, USA
Evangelos Kiountouzis, AUEB, Greece
Spyros Kokolakis, University of the Aegean, Greece
Kwok-Yan Lam, PrivyLink, Singapore
Peng Liu, The Pennsylvania State University, USA
Luigi V. Mancini, University of Rome, Italy
Juha E. Miettinen, Sonera, Finland
György Papp, VRAM Communication, Hungary
Ahmed Patel, University College Dublin, IR
Guenther Pernul, University of Essen, Germany
Francesco Pinciroli, Politecnico di Milano, Italy
Hartmut Pohl, ISIS, Germany
Reinhard Posch, Graz University of Technology, Austria
Sihan Qing, Chinese Academy of Sciences, China
Kai Rannenberg, Microsoft, United Kingdom
Indrajit Ray, Colorado State University, USA
Ravi Sandhu, George Mason University, USA
Corey D. Schou, Idaho State University, USA
E. Eugene Schultz, University of California-Berkeley Lab., USA
Gene Spafford, Purdue University, USA
Diomidis Spinellis, AUEB, Greece
Sebastiaan H. von Solms, Rand Afrikaans University, South Africa
Rossouw von Solms, Port Elizabeth Technikon, South Africa
Leon Strous, Bank of Netherlands, The Netherlands
Vijay Varadharajan, Macquarie University, Australia
Jan Vershuren, TNO-EIB, The Netherlands
Josef Vyskoc, VaF, Slovakia
Tatjana Welzer, University of Maribor, Slovenia
Louise Yngstrom, University of Stockholm, Sweden

Referees
Thodoris Balopoulos, University of the Aegean, Greece
Erik de Vink, Eindhoven University of Technology, The Netherlands
Bert den Boer, TNO-EIB, The Netherlands
Rutger Coolen, TNO-FEL, The Netherlands
Roberto Di Pietro, University of Rome, Italy
Fredj Dredi, University of Essen, Germany
Marjan Druzovec, University of Maribor, Slovenia
Antonio Durante, University of Rome, Italy
Mariki M. Eloff, University of South Africa, South Africa
Lothar Fritsch, Goethe University Frankfurt, Germany
James Frost, Idaho State University, USA
Vaibhav Gowadia, University of South Carolina, USA
John Iliadis, University of the Aegean, Greece
Alessandro Mei, University of Rome, Italy
Dina Kambouraki, Greek Data Protection Authority, Greece
Costas Lambrinoudakis, University of the Aegean, Greece
Torsten Priebel, University of Essen, Germany
Heiko Rossnagel, Goethe University Frankfurt, Germany
Sankardas Roy, George Mason University, USA
Victoria E. Skoularidou, AUEB, Greece
Andrei Stoica, University of South Carolina, USA
Suzan Thompson, TNO-EIB, The Netherlands
Meng Yu, The Pennsylvania State University, USA
Wanyu Zang, The Pennsylvania State University, USA
Sencun Zhu, George Mason University, USA

Organizing Committee
Nikolaos Kyrloglou, Athens Chamber of Commerce and Industry, Greece
Costas Lambrinoudakis, University of the Aegian, Greece
Maria Karyda, AUEB, Greece
Konstantinos Moulinos, Data Protection Commission, Greece
Dimitris Lekkas, University of the Aegean, Greece
Steven Xarhoulakos, University of the Aegean, Greece
Vasilis Tsoumas, AUEB, Greece
Lazaros P. Gymnopoulou, AUEB, Greece
IFIP/Sec'03 Workshop Program Committees

Workshop on Information Security Management

Matt Warren, Deakin University, Australia (Chair)
Steven Furnell, Plymouth University, UK
William Hutchinson, Edith Cowan University, Australia
Rossouw von Solms, Port Elizabeth Technikon, South Africa

Workshop on Privacy and Anonymity Issues in Networked and Distributed Systems

Bart De Decker, K.U.Leuven, Belgium (Co-Chair)
Els Van Herreweghen, IBM Research Lab, Switzerland (Co-Chair)
Sabrina De Capitani di Vimercati, University of Milan, Italy
Yves Deswarte, LAAS-CNRS, Toulouse, France
Hannes Federrath, University of Berlin, Germany
Simone Fischer-Hübner, Karlstad University, Sweden
Urs Gattiker, EICAR, Aalborg University, Denmark
Keith Martin, Royal Holloway, University London, UK
Refik Molva, EurÉcom, France
Andreas Pfitzmann, University of Dresden, Germany
Peter Ryan, University of Newcastle, UK
Pierangela Samarati, University of Milan, Italy
Vitay Shmatikov, SRI International, USA

Workshop on Small Systems Security

Jan Verschuren, TNO-EIB, The Netherlands (Chair)
Joan Daemen, Proton World, Belgium
Jan Elloff, Rand Afrikaans University, South Africa
Pieter Hartel, University of Twente, The Netherlands
Jaap-Henk Hoepman, Catholic University of Nijmegen, The Netherlands
Les Labuschagne, Rand Afrikaans University, South Africa
Piet Maclaine Pont, Mullpon vof, The Netherlands  
Bart Preneel, Catholic University of Leuven, Belgium  
Erik de Vink, Eindhoven University of Technology, The Netherlands

**Workshop on Security and Control of IT in Society**

*Simone Fischer-Hübner*, Karlstad University, Sweden (Co-Chair)  
*Kai Rannenberg*, Goethe University Frankfurt, Germany (Co-Chair)  
*Dagmar Brechlerova*, CUA, Czech Republic  
*Arslan Brömme*, University of Magdeburg, Germany  
*Roger Clarke*, Xamax Pty, Australia  
*Giovanni Iachello*, Georgia Inst. of Technology, USA  
*Rik Kaspersen*, Vrije Universiteit Amsterdam, The Netherlands  
*Martin Latzenhofer*, T-Mobile Austria & University of Vienna, Austria  
*Richard Sizer*, BCS, UK  
*Suzana Stojakovic-Celustka*, UZI VRH, Croatia  
*Jozef Vyskoc*, VaF, Slovakia  
* Gunnar Wenngren*, FOI - SDRA, Sweden  
*Albin Zuccato*, Karlstad University, Sweden