
SECURITY AND PRIVACY IN THE AGE OF UBIQUITOUS COMPUTING

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 UBIQUITOUS COMPUTING

*IFIP TC11 20th International Information Security Conference
May 30 – June 1, 2005, Chiba, Japan*

Edited by

Ryoichi Sasaki

*Tokyo Denki University
Japan*

Sihan Qing

*Chinese Academy of Sciences
China*

Eiji Okamoto

*University of Tsukuba
Japan*

Hiroshi Yoshiura

*University of Electro-Communications
Japan*



Springer

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 Ubiquitous Computing, Edited by Ryoichi Sasaki, Sihon Qing, Eiji Okamoto and Hiroshi Yoshiura

p.cm. (The International Federation for Information Processing)

ISBN-10: (HB) 0-387-25658-X

ISBN-13: (HB) 978-0387-25658-0

ISBN-10: (eBook) 0-387-25660-1

ISBN-13: (eBook) 978-0387-25660-3

Printed on acid-free paper.

Copyright © 2005 by International Federation for Information Processing.

All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher [Springer Science+Business Media, Inc., 233 Spring Street, New York, NY 10013, USA], except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.

The use in this publication of trade names, trademarks, service marks and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1
springeronline.com

SPIN 11418313 (HC) / 11419112 (eBook)

Contents

Preface	xi
IFIP/SEC2005 Conference Committees	xiii
PART I REGULAR PAPERS	1
Accountable Anonymous E-Mail VINCENT NAESSENS, BART DE DECKER, LIESJE DEMUYNCK	3
Protecting Consumer Data in Composite Web Services CRAIG PEARCE, PETER BERTOK, RON VAN SCHYNDEL	19
A Decision Matrix Approach ALBIN ZUCCATO	35
Assignment of Security Clearances in an Organization LECH J. JANCZEWSKI, VICTOR PORTOUGAL	51
Tool Supported Management of Information Security Culture THOMAS SCHLIENGER AND STEPHANIE TEUFEL	65
ERPSEC - A Reference Framework to Enhance Security in ERP Systems PROF. S.H. VON SOLMS, M.P. HERTENBERGER	79

A New Architecture for User Authentication and Key Exchange Using Password for Federated Enterprises	95
YANJIANG YANG, FENG BAO AND ROBERT H. DENG	
A Secure Quantum Communication Protocol Using Insecure Public Channels	113
I-MING TSAI, CHIA-MU YU, WEI-TING TU, AND SY-YEN KUO	
Trusted Component Sharing by Runtime Test and Immunization for Survivable Distributed Systems	127
JOON S. PARK, PRATHEEP CHANDRAMOHAN, GANESH DEVARAJAN, AND JOSEPH GIORDANO	
Design and Implementation of TPM SUP320	143
JIANGCHUN REN, KUI DAI, ZHIYING WANG, XUEMI ZHAO AND YUANMAN TONG	
Mathematical Models of IP Traceback Methods and Their Verification	155
KEISUKE OHMORI, AYAKO SUZUKI, MANABU OHMURO TOSHIFUMI KAI, MARIKO KAWABATA , RYU MATUSHIMA AND SHIGERU NISHIYAMA	
Transferable E-CASH Revisit	171
JOSEPH K. LIU, SANDY H. WONG [*] , DUNCAN S. WONG	
A License Transfer System for Supporting Content Portability in Digital Rights Management	189
QIONG LIU, REIHANEH SAFAVI-NAINI AND NICHOLAS PAUL SHEPPARD	
Secure Human Communications Based on Biometrics Signals	205
YONGDONG WU, FENG BAO AND ROBERT H. DENG	
Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks	223
LAURENT BUSSARD AND WALID BAGGA	
An Adaptive Polling Scheme for IEEE 802.11 Wireless LAN	239
KYUNG-JUN KIM, HYUN-SOOK KIM, SANG-DON LEE, KI-JUN HAN	

The Pairing Problem with User Interaction THOMAS PEYRIN AND SERGE VAUDENAY	251
Network Smart Card ASAD ALI, KAREN LU, AND MICHAEL MONTGOMERY	267
Protection Against Spam Using Pre-Challenges RODRIGO ROMAN, JIANYING ZHOU, AND JAVIER LOPEZ	281
Automatically Hardening Web Applications Using Precise Tainting ANH NGUYEN-TUONG, SALVATORE GUARNIERI, DOUG GREENE, JEFF SHIRLEY, DAVID EVANS	295
Traffic Redirection Attack Protection System (TRAPS) VRIZLYNN L. L. THING, HENRY C. J. LEE AND MORRIS SLOMAN	309
Statistical Signatures for Early Detection of Flooding Denial-of-service Attacks JOHN HAGGERTY, QI SHI AND MADJID MERABTI	327
Design, Implementation, and Evaluation of FRiTrace WAYNE HUANG, J.L. CONG, CHIEN-LONG WU, FAN ZHAO, S. FELIX WU	343
Design and Implementation of a High-Performance Network Intrusion Prevention System KONSTANTINOS XINIDIS, KOSTAS G. ANAGNOSTAKIS, EVANGELOS P. MARKATOS	359
STRIDE: Polymorphic Sled Detection through Instruction Sequence Analysis P. AKRITIDIS, E. P. MARKATOS, M. POLYCHRONAKIS, AND K. ANAGNOSTAKIS	375
PIRANHA: Fast and Memory-Efficient Pattern Matching for Intrusion Detection S. ANTONATOS, M. POLYCHRONAKIS, P. AKRITIDIS, K.G. ANAGNOSTAKIS AND E.P. MARKATOS	393
Designated-Verifier Proxy Signature Schemes GUILIN WANG	409

Tripartite Concurrent Signatures WILLY SUSILO AND YI MU	425
Signcryption in Hierarchical Identity Based Cryptosystem SHERMAN S.M. CHOW, TSZ HON YUEN, LUCAS C.K. HUI, AND S.M. YIU	443
Protecting Group Dynamic Information in Large Scale Multicast Groups YONGDONG WU, TIEYAN LI, AND ROBERT H. DENG	459
Secure Group Communication with Distributed Generation of Private Keys for Ad-hoc Networks SHRIKANT SUNDARAM, PETER BERTOK AND BENJAMIN BURTON	477
Ensuring Media Integrity on Third-party Infrastructures JANA DITTMANN, STEFAN KATZENBEISSER, CHRISTIAN SCHALLHART, HELMUT VEITH	493
A New Fragile Mesh Watermarking Algorithm for Authentication HAO-TIAN WU AND YIU-MING CHEUNG	509
New Paradigm in Graph-based Visual Secret Sharing Scheme by Accepting Reversal in Black-White Images YUJI SUGA	525
PART II WORKSHOP PAPERS	537
Overcoming Channel Bandwidth Constraints in Secure SIM Applications JOHN A. MACDONALD, WILLIAM SIRETT AND CHRIS J. MITCHELL	539
On the Performance of Certificate Revocation Protocols Based on a Java Card Certificate Client Implementation K. PAPAPANAGIOTOU, K. MARKANTONAKIS, Q. ZHANG, W.G. SIRETT AND K. MAYES	551
On-the-Fly Formal Testing of a Smart Card Applet ARJEN VAN WEELDEN, MARTIJN OOSTDIJK, LARS FRANTZEN, PIETER KOOPMAN, JAN TRETSMANS	565

A Computationally Feasible SPA Attack on AES via Optimized Search JOEL VANLAVEN, MARK BREHOB, AND KEVIN J. COMPTON	577
The Proof by $2m-1$: A Low-cost Method to Check Arithmetic Computations SYLVAIN GUILLEY AND PHILIPPE HOOGVORST	589
Streamto: Streaming Content Using a Tamper-Resistant Token JIEYIN CHENG, CHEUN NGEN CHONG, JEROEN M. DOUMEN, SANDRO ETALLE, PIETER H. HARTEL AND STEFAN NIKOLAUS	601

Preface

This book contains the proceedings of the 20th IFIP International Information Security Conference (IFIP/SEC2005) held from 30th May to 1st June, 2005 in Chiba, Japan. It was the 20th SEC conference in the history of IFIP TC-11. The first one was held in Stockholm, Sweden in May 1983. After that, IFIP/SEC conferences have been in various countries all over the world. The last IFIP/SEC conference held in Asia was IFIP/SEC2000 in Beijing, China.

In IFIP/SEC2005, we emphasize on “Security and Privacy in the Age of Ubiquitous Computing”. Even in the age of ubiquitous computing, the importance of the Internet will not change and we still need to solve conventional security issues. Moreover, we need to deal with the new issues such as security in P2P environment, privacy issues in the use of smart cards and RFID systems. Therefore, in IFIP/SEC2005, we have included a workshop “Small Systems Security and Smart Cards” and a panel session “Security in Ubiquitous Computing”.

This book includes the papers selected for presentation at IFIP/SEC2005 as well as the associated workshop. In response to the call for papers, 124 papers were submitted to the main conference track. These papers were evaluated by members of the Program Committee in terms of their relevance, originality, significance, technical quality and presentation. From the submitted papers, 34 were selected for presentation at the conference (an acceptance rate of 27%). We also include 6 short papers selected by the Workshop committee.

We would like to thank Mr. Leon Strous, chair of IFIP TC-11, Professor Norihisa Doi, Professor Hideki Imai, Professor Tsuneo Kurokawa and Professor Shigeo Tsujii,

members of the SEC2005 Advisory Committee for their continuous advice. We are grateful to the members of the Program Committee for their voluntary efforts to review manuscripts. We are also grateful to the members of the Local Organizing Committee for their efforts in preparing this conference, especially Professor Yuko Murayama, chair of this committee.

Ryoichi Sasaki, Tokyo Denki University
(General Chair)

Sihan Qing, Chinese Academy of Science

Eiji Okamoto, University of Tsukuba

(Program Chairs)

IFIP/SEC2005 Conference Committees

Conference General Chair

Ryoichi Sasaki, Tokyo Denki University, Japan

Advisory Committee

Norihisa Doi, Chuo University, Japan

Hideki Imai, University of Tokyo, Japan

Tsuneo Kurokawa, Kokugakuin University, Japan

Shigeo Tsujii, Chuo University, Japan

Programme Committee co-Chairs

Si-han Qing, Chinese Academy of Sciences, China

Eiji Okamoto, University of Tsukuba, Japan

Programme Committee

H. Armstrong, Curtin University of Technology, Australia

W. Caelli, Queensland University of Technology, Australia

E. Chaparro, Fundacion Via Libre, Argentina

B. de Decker, K. U. Leuven, Belgium

Y. Deswarte, LAAS-CNRS, France

M. Dupuy, SGDN/DCSSI/CERTA, France

M. El-Hadidi, Cairo University, Egypt

J. Eloff, University of Pretoria, South Africa

S. Fischer-Huebner, Karlstad University, Sweden

- D. Gollmann, Technische Universität Hamburg-Harburg, Germany
D. Gritzalis, Athens University of Economics and Business, Greece
H. Inaba, Kyoto Institute of Technology, Japan
K. Iwamura, Canon Inc., Japan
S. Jajodia, George Mason University, USA
S. Katsikas, University of the Aegean, Greece
H. Kikuchi, Tokai University, Japan
K.-Y. Lam, PrivyLink, Singapore
C. Landwehr, CISE/CNS, USA
W. List, Partner, Independent, UK
J. Lopez, University of Malaga, Spain
K. Matsuura, University of Tokyo, Japan
Y. Murayama, Iwate Prefectural University, Japan
T. Nakanishi, Okayama University, Japan
M. Nishigaki, Shizuoka University, Japan
G. Papp, Vodafone Hungary, Hungary
M. Park, Mitsubishi Electronic Corporation, Japan
H. Pohl, ISIS - InStitute for Information Security, Germany
R. Posch, Graz Univ. of Technology, Austria
K. Rannenber, Goethe University Frankfurt, Germany
K. Sakurai, Kyushu University, Japan
P. Samarati, University of Milan, Italy
I. Schaumuller-Bichl, Johann Wilhelm Kleinstrasse 11, Austria
L. Strous, De Nederlandsche Bank, NL
K. Tanaka, Shinshu University, Japan
S. Teufel, Universite de Fribourg, Switzerland
D. Tygar, University of California, Berkeley, USA
V. Varadharajan, Macquarie Univ., Australia
I. Verschuren, TNO ITSEF, NL
J. Vyskoc, VaF, Slovakia
M. Warren, Deakin University, Australia
T. Welzer, University of Maribor, Slovenia
H. Yoshiura, University of Electro-Communications, Japan
S. Furnell, University of Plymouth, UK
J. Knudsen, Copenhagen Hospital Corporation, Denmark
I. Ray, Colorado State University, USA
T. Virtanen, Helsinki University of Technology, Finland
R. Solms, Port Elizabeth Technikon, South Africa
Local Organizing Committee Chair
Yuko Murayama, Iwate Prefectural University, Japan

Local Organizing Committee

Steering Chairs

Yuko Murayama, Iwate Prefectural University, Japan
Yoshito Tobe, Tokyo Denki University, Japan

Program Chairs

Eiji Okamoto, Tsukuba University, Japan
Hiroshi Yoshiura, University of Electro-Communication, Japan
Mi Rang Park, Mitsubishi Electronic Corporation, Japan

Finance Chair

Masatoshi Terada, Hitachi Limited, Japan

Publicity Chairs

Masakatsu Nishigaki, Shizuoka University, Japan
Ryuya Uda, Tokyo University of Technology, Japan

Local Arrangement Chairs

Hiroaki Kikuchi, Tokai University, Japan
Moriaki Itazu, Tokyo Denki University, Japan

Publication Chair

Kanta Matsuura, University of Tokyo, Japan

Liaison Chairs

Seiichiro Hayashi, Japan Internet Payment Promotion Association,
Japan
Kouji Nakao, KDDI Corporation, Japan
Satoru Torii, Fujitsu Limited, Japan

Workshop on Small Systems Security and Smart Cards

Working Conference Programme Committee

Jean-Jacques Quisquater, UCL, Belgium
Jan Verschuren, TNO ITSEF-BV, The Netherlands,
Joan Daemen, STMicroelectronics, Belgium
Jan Eloff, University of Pretoria, South Africa
Pieter Hartel, Twente University, The Netherlands
Jaap-Henk Hoepman, University of Nijmegen, The Netherlands
Les Labuschagne, RAU Standard Bank Academy for Information
Technology, South Africa
Piet Maclaine Pont, Mullpon vof, The Netherlands
Michael Montgomery, Axalto Schlumberger, USA
Pierre Paradinas, CNAM, Paris, France
Erik Poll, University of Nijmegen, The Netherlands
Ingrid Verbauwhede, KU Leuven, Belgium
Erik de Vink, Eindhoven University of Technology, The Netherlands
Bert den Boer, Independent Cryptographer, The Netherlands
Jeroen Doumen, Twente University, The Netherlands