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, Sihan 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.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1 SPIN 11418313 (HC) / 11419112 (eBook)
springeronline.com

Contents

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
Sihan 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 Universitat 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. Rannenberg, Goethe University Frankfurt, Germany
K. Sakurai, Kyushu University, Japan
P. Samarati, University of Milan, Italy
I. Schaumuller-Bichl, Johann Wilhelm Kleinstrase 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, Macquire 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