

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Germany

Madhu Sudan

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbruecken, Germany

Jan Camenisch Valentin Kisimov
Maria Dubovitskaya (Eds.)

Open Research Problems in Network Security

IFIP WG 11.4 International Workshop, iNetSec 2010
Sofia, Bulgaria, March 5-6, 2010
Revised Selected Papers

Volume Editors

Jan Camenisch
Maria Dubovitskaya
IBM Research Zurich, Säumerstr. 4
8803 Rüschlikon, Switzerland
E-mail: {jca, mdu}@zurich.ibm.com

Valentin Kisimov
University of National and World Economy
Studentski Grad "Hr. Botev", 1700 Sofia, Bulgaria
E-mail: vkisimov@gmail.com

ISSN 0302-9743
ISBN 978-3-642-19227-2
DOI 10.1007/978-3-642-19228-9
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-19228-9

Library of Congress Control Number: 2011920837

CR Subject Classification (1998): K.6.5, K.4, C.2, E.3, D.4.6, H.3.4-5

LNCS Sublibrary: SL 4 – Security and Cryptology

© IFIP International Federation for Information Processing 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

iNetSec 2010 is the main conference of working group WG 11.4 of IFIP. Originally, the conference was run in the traditional format where research papers get submitted, peer-reviewed, and then presented at the conference. Because there are (far too) many security conferences like that, it was decided in 2009 to change the format into a forum for the discussion of open research problems and directions in network security.

To enable this more open style, while still remaining focused on particular topics, we called for two-page abstracts in which the authors were asked to outline an open research problem or direction. These abstracts were reviewed by the entire program committee who ranked each of them according to whether the problem presented was relevant and suited for a discussion. Based on this, about half of the submitted abstracts were chosen for presentation and discussion at the conference. The authors were asked to later write and submit full papers based on their abstracts and the discussions at the workshop. These are the papers that you are now holding in your hands.

The conference also hosted two invited talks. Basie von Solms (President of IFIP) argued in his talk entitled “Securing the Internet: Fact or Fiction?” that secure computer networks are an illusion with which we have to cope. The paper to the talk is also contained in these proceedings. Leon Straus (President Elect of IFIP) shared his insights on “Network and Infrastructure Research Needs from a Financial Business Perspective” which showed how much research can and should learn from practitioners from all fields using computer technologies.

On the last day of the conference, the attendees gathered in a lively discussion about security and cloud computing that opened the eyes of quite a few. The social highlights of the conference were the Bulgarian dinner accompanied by traditional live music and a guided tour through Sofia that despite the freezing temperature was delightful and impressive.

We are grateful to the two invited speakers, the authors, the PC members, and last but certainly not least, the local organizing committee.

September 2010

Jan Camenisch
Valentin Kisimov

iNetSec 2010

Open Research Problems in Network Security

University of National and World Economy, Sofia, Bulgaria

March 5-6, 2010

Organized in cooperation with *IFIP WG 11.4*

Executive Committee

| | |
|------------------|--------------------------------------|
| Program Chair | Jan Camenisch, IBM Research – Zurich |
| Organizing Chair | Valentin Kisimov, UNWE |

Program Committee

| | |
|-----------------------|----------------------------|
| Jan Camenisch | IBM Research |
| Virgil Gligor | Carnegie Mellon University |
| Jean-Pierre Hubaux | EPFL |
| Simone Fischer-Hübner | Karlstad University |
| Dogan Kesdogan | University of Siegen |
| Valentin Kisimov | UNWE |
| Albert Levi | Sabancı University |
| Javier Lopez | University of Malaga |
| Refik Molva | Eurecom |

Local Organizing Committee

| | |
|-------------------|-----------------|
| Valentin Kisimov | IFIP TC11, UNWE |
| Dimiter Velev | UNWE |
| Kamelia Stefanova | UNWE |
| Vanya Lazarova | UNWE |

Table of Contents

Invited Talk and Scheduling

| | |
|--|---|
| Securing the Internet: Fact or Fiction? | 1 |
| <i>Basie von Solms</i> | |
| Open Research Questions of Privacy-Enhanced Event Scheduling | 9 |
| <i>Benjamin Kellermann</i> | |

Adversaries

| | |
|---|----|
| Event Handoff Unobservability in WSN | 20 |
| <i>Stefano Ortolani, Mauro Conti, Bruno Crispo, and Roberto Di Pietro</i> | |
| Emerging and Future Cyber Threats to Critical Systems | 29 |
| <i>Edita Djambazova, Magnus Almgren, Kiril Dimitrov, and Erland Jonsson</i> | |
| Adversarial Security: Getting to the Root of the Problem | 47 |
| <i>Raphael C.-W. Phan, John N. Whitley, and David J. Parish</i> | |
| Practical Experiences with Purenet, a Self-learning Malware Prevention System | 56 |
| <i>Alapan Arnab, Tobias Martin, and Andrew Hutchison</i> | |
| A Biometrics-Based Solution to Combat SIM Swap Fraud | 70 |
| <i>Louis Jordaan and Basie von Solms</i> | |
| Are BGP Routers Open to Attack? An Experiment | 88 |
| <i>Ludovico Cavedon, Christopher Kruegel, and Giovanni Vigna</i> | |

Secure Processes

| | |
|--|-----|
| Securing the Core University Business Processes | 104 |
| <i>Veliko Ivanov, Monika Tzaneva, Alexandra Murdjeva, and Valentin Kisimov</i> | |
| Some Technologies for Information Security Protection in Weak-Controlled Computer Systems and Their Applicability for eGovernment Services Users | 117 |
| <i>Anton Palazov</i> | |

| | |
|--|-----|
| Real-Time System for Assessing the Information Security of Computer Networks | 123 |
| <i>Dimitrina Polimirova and Eugene Nickolov</i> | |
| Evidential Notions of Defensibility and Admissibility with Property Preservation | 134 |
| <i>Raphael C.-W. Phan, Ahmad R. Amran, John N. Whitley, and David J. Parish</i> | |
| Security for Clouds | |
| Cloud Infrastructure Security | 140 |
| <i>Dimiter Velez and Plamena Zlateva</i> | |
| Security and Privacy Implications of Cloud Computing – Lost in the Cloud | 149 |
| <i>Vassilka Tchiflionova</i> | |
| The Need for Interoperable Reputation Systems | 159 |
| <i>Sandra Steinbrecher</i> | |
| Author Index | 171 |