Lecture Notes in Computer Science 7161

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Peeter Laud (Ed.)

Information Security Technology for Applications

16th Nordic Conference on Secure IT Systems, NordSec 2011
Tallinn, Estonia, October 26-28, 2011
Revised Selected Papers

Volume Editor

Peeter Laud
Cybernetica AS
Ülikooli 2
51003 Tartu, Estonia
E-mail: peeter@cyber.ee

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-29614-7 e-ISBN 978-3-642-29615-4
DOI 10.1007/978-3-642-29615-4
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012935688

CR Subject Classification (1998): D.4.6, K.6.5, D.2, H.2.7, K.4.4, E.3, C.2

LNCS Sublibrary: SL 4 – Security and Cryptology

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

These are the conference proceedings of NordSec 2011, the 16th Nordic Conference on Secure IT-Systems. They contain the revised versions of the full papers that were accepted and presented at the conference, which took place during October 26–28, 2011, in Tallinn, Estonia.

The NordSec workshops were started in 1996 with the aim of bringing together researchers and practitioners within computer security in the Nordic countries, thereby establishing a forum for discussions and co-operation between universities, industry and computer societies. Since then, the workshop has developed into a fully fledged international information security conference, held in the Nordic countries on a round robin basis.

This year, the conference accepted contributions in the form of full papers, short papers, and posters. Full papers were solicited for mature results, short papers for ongoing work, and posters as a form of student contribution. We received a total of 51 valid paper submissions, among them 8 submissions as short papers. The Program Committee tried to give at least three reviews to all submissions. Out of the submitted papers, 16 were accepted as full papers and 8 as short papers. Also, some full submissions were accepted as short papers. In addition to the talks by the authors of accepted papers, we also had two invited talks by Estonian e-governance and security specialists. In their talks, they analyzed some of the most-used and highest-profile information systems for the Estonian e-government — the *X-road* middleware and the Internet voting system.

Since 2008, Nordsec conferences have been happy to welcome the participation of the Second-year students of the international Erasmus Mundus master's programme "NordSecMob" in security and mobile computing. The students are encouraged to participate in the conference by submitting posters reporting on work they have performed. This year, six posters were submitted and presented at the conference.

Even though NordSec is not a large conference, the efforts of many people are necessary for its successful organization. We would like to thank everybody who made the conference possible. We thank the Program Committee for reviewing the papers and discussing them, thereby creating the best possible program for the conference. We thank the subreviewers for the extra help they gave us with the reviews. We also thank the Poster Chair for helping the students to produce high-quality posters for the conference, and the invited speakers for agreeing to share their insights. And obviously, we are thankful to all the authors for submitting their papers for consideration of the program committee because, without those, there would not have been anything in the conference program.

We are especially grateful to the Organizing Committee of the conference. Making sure that all the tiny details are taken care of is a lot of work, and we heartfully thank Imbi, Liina, and Madeline for that.

We are also grateful to Cybernetica AS for agreeing to host the conference, and to the Estonian Centre of Excellence in Computer Science, EXCS (financed through the European Regional Development Fund) for providing financial support.

November 2011 Peeter Laud

Organization

General Chair

Peeter Laud	Cybernetica AS and University of Tartu, Estonia

Program Committee

Frederik Armknecht	University of Mannheim, Germany
Lizzie Coles-Kemp	Royal Holloway, University of London, UK
Mads Dam	KTH Royal Institute of Technology, Sweden
Simone Fischer-Hübner	Karlstad University, Sweden
Dieter Gollmann	Hamburg University of Technology (TUHH), Germany
Erland Jonsson	Chalmers University of Technology, Sweden
Svein Johan Knapskog	Norwegian University of Science and Technology, Norway
Igor Kotenko	St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia
Helger Lipmaa	University of Tartu, Estonia
Fabio Massacci	University of Trento, Italy
Chris Mitchell	Royal Holloway, University of London, UK
Kaisa Nyberg	Aalto University, Finland
Kai Rannenberg	Goethe University, Frankfurt, Germany
Heiko Roßnagel	Fraunhofer IAO, Germany
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Jaak Tepandi	Tallinn University of Technology, Estonia
Dominique Unruh	University of Tartu, Estonia
Risto Vaarandi	Cooperative Cyber Defense Centre of Excellence, Estonia
Jan Willemson	Cybernetica AS, Estonia
Ender Yüksel	Technical University of Denmark, Denmark

Poster Chair

Margus Niitsoo	University of Tartu, Estonia

Organizing Committee

Madeline González Muñiz
Liina Kamm
Imbi Nõgisto

Reviewers

Goekhan Bal
Musard Balliu
Alberto Battocchi
Nataliia Bielova
Arnar Birgisson
Laura Boffi
Andrey Chechulin
Vasily Desnitsky
Andre Deuker
Vassil Dimitrov
Olga Gadyatskaya
Paolo Guarda
Matúš Harvan
Daniel Hedin
Marvin Hegen
Stephan Heim
Kimmo Järvinen
Dmitriy Komashinskiy
Alexey Konovalov
Gurvan Le Guernic
Andreas Lundblad
Jonas Magazinius
Raimundas Matulevičius
Vasily Mikhalev
Azalia Mirhoseini
Viet Hung Nguyen
Valtteri Niemi
Tomas Olovsson
Federica Paci
Tobias Pulls
Willard Rafnsson
Andrea Röck
Shokrollahi
Lars Wolos
Bingsheng Zhang
Jan Zibuschka

Table of Contents

Invited Papers

Contributed Papers