Lecture Notes in Computer Science 7127

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

Tuomas Aura Kimmo Järvinen
Kaisa Nyberg (Eds.)

Information Security Technology for Applications

15th Nordic Conference on Secure IT Systems,
NordSec 2010
Espoo, Finland, October 27-29, 2010
Revised Selected Papers

Springer

Volume Editors

Tuomas Aura
Kimmo Järvinen
Kaisa Nyberg
Aalto University
School of Science
Konemiehentie 2, 02150 Espoo, Finland
E-mail: {tuomas.aura, kimmo.jarvinen, kaisa.nyberg}@aalto.fi

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-27936-2 e-ISBN 978-3-642-27937-9
DOI 10.1007/978-3-642-27937-9
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011945062

CR Subject Classification (1998): D.4.6, K.6.5, D.2, H.2.7, K.4.2, 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

The Nordsec workshops started in 1996 with the aim of bringing together computer security researchers and practitioners from the Nordic countries. The event focuses on applied IT security and, from the beginning, its goal has been to encourage interaction between academic and industrial research. Over the years, Nordsec has developed into an international conference that takes place in the Nordic countries on a round-robin basis. It has also become a key meeting venue for Nordic university teachers and students with an interest in security research.

The 15th Nordic Conference in Secure IT Systems took place at Aalto University in Finland during October 27–29, 2010. The program of this year's conference was a cross-section of the security research at Nordic universities and industrial research centers with some contributions from around Europe. The themes ranged from the enforcement of security policies to security monitoring and network security. There were also papers on privacy, cryptography, and security protocol implementation. The conference received 37 submissions, of which 13 were accepted for presentation as full papers and three as short papers. In the original workshop spirit, the authors were able to revise their papers based on discussions at the conference.

The keynote talk at Nordsec was given by Erka Koivunen from CERT-FI with the title "Why Wasn't I Notified?": Information Security Incident Handling Demystified. An invited paper based on the talk is included in the proceedings. Furthermore, a large number of students presented their work at a poster session and competition.

The proceedings also include three selected papers from the OWASP AppSec Research 2010 conference, which focuses on Web application security. These papers were originally presented in Stockholm during June 21–24, 2010. The authors of the selected papers were invited to submit revised papers for a joint conference publication and to give talks at Nordsec.

We would like to thank the authors, members of the Program Committee, reviewers, students presenting posters, the Organizing Committee, and all conference attendees for coming together and making Nordsec 2010 a successful scientific and social event for both security researchers and practitioners.

October 2011

Tuomas Aura
Kimmo Järvinen
Kaisa Nyberg

Organization

Nordsec 2010
October 27–29, 2010, Espoo, Finland

Program Chairs

Tuomas Aura	Aalto University, Finland
Kaisa Nyberg	Aalto University and Nokia Research Center, Finland

Local Organizing Committee

Tuomas Aura	Aalto University, Finland
Kimmo Järvinen	Aalto University, Finland

Program Committee

N. Asokan	Nokia Research Center, Finland
Tuomas Aura	Aalto University, Finland
Catharina Candolin	Finnish Defence Forces, Finland
Mads Dam	Royal Institute of Technology, Sweden
Simone Fischer-Hübner	Karlstad University, Sweden
Viiveke Fåk	Linköping University, Sweden
Dieter Gollmann	Hamburg University of Technology, Germany
Christian Damsgaard Jensen	Technical University of Denmark, Denmark
Erland Jonsson	Chalmers University of Technology, Sweden
Svein Johan Knapskog	Norwegian University of Science and Technology, Norway
Audun Jøsang	University of Oslo, Norway
Peeter Laud	Cybernetica AS and University of Tartu, Estonia
Helger Lipmaa	Tallinn University, Estonia
Vaclav Matyas	Masaryk University, Czech Republic
Chris Mitchell	Royal Holloway, University of London, UK
Kaisa Nyberg	Aalto University and Nokia Research Center, Finland
Christian W. Probst	Technical University of Denmark, Denmark
Hanne Riis Nielson	Technical University of Denmark, Denmark

Michael Roe	University of Hertfordshire, UK
Nahid Shahmehri	Linköping University, Sweden
Einar Snekkenes	Norwegian Information Security Lab, Norway
Alf Zugenmaier	Munich University of Applied Sciences, Germany

Reviewers

Naveed Ahmed	Hans Hedbom
Waleed Alrodhan	Aapo Kalliola
Musard Balliu	Atefeh Mashatan
Stefan Berthold	Davide Papini
Joo Yeon Cho	Emilia Käsper
Nicola Dragoni	Andrea Röck
Olof Hagsand	Ge Zhang

Table of Contents

Policy Enforcement

Selected OWASP AppSec Research 2010 Papers

Cryptography and Protocols