

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

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

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
ISBN 978-3-642-27936-2
DOI 10.1007/978-3-642-27937-9
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349
e-ISBN 978-3-642-27937-9

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

© Springer-Verlag Berlin Heidelberg 2012

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

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

VIII Organization

Michael Roe
Nahid Shahmehri
Einar Snekkenes
Alf Zugenmaier

University of Hertfordshire, UK
Linköping University, Sweden
Norwegian Information Security Lab, Norway
Munich University of Applied Sciences,
Germany

Reviewers

Naveed Ahmed
Waleed Alrodhan
Musard Balliu
Stefan Berthold
Joo Yeon Cho
Nicola Dragoni
Olof Hagsand

Hans Hedbom
Aapo Kalliola
Atefeh Mashatan
Davide Papini
Emilia Käsper
Andrea Röck
Ge Zhang

Table of Contents

Network Security

BloomCasting: Security in Bloom Filter Based Multicast	1
<i>Mikko Särelä, Christian Esteve Rothenberg, András Zahemszky, Pekka Nikander, and Jörg Ott</i>	
Authentication Session Migration	17
<i>Sanna Suoranta, Jani Heikkinen, and Pekka Silvekoski</i>	
Mitigation of Unsolicited Traffic across Domains with Host Identities and Puzzles	33
<i>Miika Komu, Sasu Tarkoma, and Andrey Lukyanenko</i>	
Experimental Analysis of the Femtocell Location Verification Techniques (Short Paper)	49
<i>Ravishankar Borgaonkar, Kevin Redon, and Jean-Pierre Seifert</i>	

Invited Talk

“Why Wasn’t I Notified?”: Information Security Incident Reporting Demystified	55
<i>Erka Koivunen</i>	

Monitoring and Reputation

Use of Ratings from Personalized Communities for Trustworthy Application Installation	71
<i>Pern Hui Chia, Andreas P. Heiner, and N. Asokan</i>	
Practical Private Information Aggregation in Large Networks	89
<i>Gunnar Kreitz, Mads Dam, and Douglas Wikström</i>	
Tracking Malicious Hosts on a 10Gbps Backbone Link	104
<i>Magnus Almgren and Wolfgang John</i>	

Privacy

Service Users’ Requirements for Tools to Support Effective On-line Privacy and Consent Practices	121
<i>Elahe Kani-Zabihi and Lizzie Coles-Kemp</i>	

Analyzing Characteristic Host Access Patterns for Re-identification of Web User Sessions	136
<i>Dominik Herrmann, Christoph Gerber, Christian Banse, and Hannes Federrath</i>	

Policy Enforcement

A Framework for the Modular Specification and Orchestration of Authorization Policies	155
<i>Jason Crampton and Michael Huth</i>	
Credential Disabling from Trusted Execution Environments	171
<i>Kari Kostiaainen, N. Asokan, and Jan-Erik Ekberg</i>	
Java Card Architecture for Autonomous Yet Secure Evolution of Smart Cards Applications (Short Paper)	187
<i>Olga Gadyatskaya, Fabio Massacci, Federica Paci, and Sergey Stankevich</i>	
Implementing Erasure Policies Using Taint Analysis	193
<i>Filippo Del Tedesco, Alejandro Russo, and David Sands</i>	

Selected OWASP AppSec Research 2010 Papers

A Taint Mode for Python via a Library	210
<i>Juan José Conti and Alejandro Russo</i>	
Security of Web Mashups: A Survey	223
<i>Philippe De Ryck, Maarten Decat, Lieven Desmet, Frank Piessens, and Wouter Joosen</i>	
Safe Wrappers and Sane Policies for Self Protecting JavaScript	239
<i>Jonas Magazinius, Phu H. Phung, and David Sands</i>	

Cryptography and Protocols

Protocol Implementation Generator	256
<i>Jose Quaresma and Christian W. Probst</i>	
Secure and Fast Implementations of Two Involution Ciphers	269
<i>Billy Bob Brumley</i>	
The PASSERINE Public Key Encryption and Authentication Mechanism (Short Paper)	283
<i>Markku-Juhani O. Saarinen</i>	

Author Index	289
---------------------------	-----