

*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*

Audun Jøsang Bengt Carlsson (Eds.)

# Secure IT Systems

17th Nordic Conference, NordSec 2012  
Karlskrona, Sweden, October 31 – November 2, 2012  
Proceedings

Volume Editors

Audun Jøsang  
University of Oslo  
Gaustadalléen 23b, 0373 Oslo, Norway  
E-mail: josang@mn.uio.no

Bengt Carlsson  
Blekinge Institute of Technology  
Valhallavägen 1, 37179 Karlskrona, Sweden  
E-mail: bengt.carlsson@bth.se

ISSN 0302-9743 e-ISSN 1611-3349  
ISBN 978-3-642-34209-7 e-ISBN 978-3-642-34210-3  
DOI 10.1007/978-3-642-34210-3  
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012949091

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

© 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

These proceedings contain the full papers presented at NordSec 2012, the 17th Nordic Conference on Secure IT Systems, held at Blekinge Institute of Technology in Karlskrona, Sweden, during 31 October – 2 November 2012.

NordSec was initially started in 1996 as a workshop series with the aim of bringing together researchers and practitioners working on 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.

NordSec 2012 solicited contributions in the form of full papers presenting mature work, short papers presenting ongoing work, and student posters. We received a total of 32 valid submissions of full papers, each of which was reviewed by at least three Program Committee members. Out of the submitted full papers, 16 were accepted for presentation at the conference. Also, some submitted full papers were accepted as short papers published in locally printed proceedings.

Since 2008, Nordsec has welcomed the participation of 2nd-year students of the international Erasmus Mundus Masters programme “NordSecMob”, as well as other master’s students in IT security, to present posters that show work done as part of their master’s studies. The students’ fresh and often radical ideas stimulate very interesting discussions among NordSec participants.

The combined effort of many people was needed for the organization of NordSec 2012, and we would like to give recognition to all who contributed to making the conference a success. 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. Most importantly we are thankful to all the authors who submitted their papers to NordSec 2012, and to the conference attendees who took part in the discussions during the conference. Many other people also contributed in some way to the organization of NordSec 2012. We are also grateful to Blekinge Institute of Technology for allowing the conference to use its facilities, and to NetPort Karlshamn for sponsoring the welcome reception. As a result of your great efforts and contributions, NordSec continues to be a valuable meeting place for the information security community.

October 2012

Bengt Carlsson  
Audun Jøsang



Radu Lupu	Politehnica University of Bucharest, Romania
Fabio Massacci	University of Trento, Italy
Sjouke Mauw	University of Luxembourg
Wojciech Mazurczyk	Warsaw University of Technology, Poland
Chris Mitchell	Royal Holloway College, UK
Simin Nadjm-Tehrani	Linköping University, Sweden
Kaisa Nyberg	Helsinki University of Technology, Finland
Lars Olaussen	Norwegian Security Authority
Jon Ølnes	Unibridge, Norway
Jakob Illeborg Pagter	The Alexandra Institute Ltd., Denmark
Marina Papatriantafylou	Chalmers University of Technology, Sweden
Christian W. Probst	Technical University of Denmark
Kai Rannenber	Goethe University Frankfurt, Germany
Christian Rohner	Uppsala University, Sweden
Heiko Roßnagel	Fraunhofer IAO, Germany
Sini Ruohomaa	University of Helsinki, Finland
Andrei Sabelfeld	Chalmers University of Technology, Sweden
Anne-Karen Seip	The Financial Supervisory Authority of Norway
Bjørnar Solhaug	SINTEF, Norway
Teodor Sommestad	Swedish Defence Research Agency
Nils Kalstad Svendsen	Gjøvik University College, Norway
Jaak Tepandi	Tallinn University of Technology, Estonia
Dominique Unruh	Saarland University, Germany
Risto Vaarandi	NATO Coop. Cyber Defence Centre, Estonia
Bjørn Victor	Uppsala University, Sweden
Ymir Vigfusson	IBM Research Haifa, Israel
Benedikt Westermann	Norwegian University of Technology
Jan Willemson	Cybernetica Ltd., Estonia
Ender Yüksel	Technical University of Denmark

## Subreviewers

Hugo Jonker	Andreas Leicher	Daniel Hedin
Tobias Pulls	Bart van Delft	Goekhan Bal
Vasily Mikhalev	Jun Pang	Fatbardh Veseli
Bingsheng Zhang	Hamid Ebadi	Jan Zibuschka
Sebastian Kurowski	Arnar Birgisson	
Sandeep Tamrakar	Musard Balliu	

## Sponsoring Institutions

NetPort Karlshamn	<a href="http://www.netport.se/">http://www.netport.se/</a>
Blekinge Institute of Technology	<a href="http://www.bth.se/">http://www.bth.se/</a>

# Table of Contents

## Application Security

Designed to Fail: A USB-Connected Reader for Online Banking . . . . .	1
<i>Arjan Blom, Gerhard de Koning Gans, Erik Poll, Joeri de Ruiter, and Roel Verdult</i>	
Security Add-Ons for Mobile Platforms . . . . .	17
<i>Benjamin Adolphi and Hanno Langweg</i>	
THAPS: Automated Vulnerability Scanning of PHP Applications . . . . .	31
<i>Torben Jensen, Heine Pedersen, Mads Chr. Olesen, and René Rydhof Hansen</i>	

## Security Management

Cyber Security Exercises and Competitions as a Platform for Cyber Security Experiments . . . . .	47
<i>Teodor Sommestad and Jonas Hallberg</i>	
The Development of Cyber Security Warning, Advice and Report Points . . . . .	61
<i>Tony Proctor</i>	
Towards an Empirical Examination of IT Security Infrastructures in SME . . . . .	73
<i>Ramona Groner and Philipp Brune</i>	
How to Select a Security Requirements Method? A Comparative Study with Students and Practitioners . . . . .	89
<i>Fabio Massacci and Federica Paci</i>	

## System Security

There Is Safety in Numbers: Preventing Control-Flow Hijacking by Duplication . . . . .	105
<i>Job Noorman, Nick Nikiforakis, and Frank Piessens</i>	
Coinductive Unwinding of Security-Relevant Hyperproperties . . . . .	121
<i>Dimitar Milushev and Dave Clarke</i>	
Retooling and Securing Systemic Debugging . . . . .	137
<i>Björn Ståhl and Per Mellstrand</i>	

## Network Security

Cracking Associative Passwords . . . . .	153
<i>Kirsi Helkala, Nils Kalstad Svendsen, Per Thorsheim, and Anders Wiehe</i>	
A Hybrid Approach for Highly Available and Secure Storage of Pseudo-SSO Credentials . . . . .	169
<i>Jan Zibuschka and Lothar Fritsch</i>	
Assessing the Quality of Packet-Level Traces Collected on Internet Backbone Links . . . . .	184
<i>Behrooz Sangchoolie, Mazdak Rajabi Nasab, Tomas Olovsson, and Wolfgang John</i>	

## Trust Management

Everything But the Kitchen Sink: Determining the Effect of Multiple Attacks on Privacy Preserving Technology Users . . . . .	199
<i>Jason W. Clark</i>	
Can We Identify Manipulative Behavior and the Corresponding Suspects on Review Websites Using Supervised Learning? . . . . .	215
<i>Huiying Duan and Cécilia Zirn</i>	
Privacy-Friendly Cloud Storage for the Data Track: An Educational Transparency Tool . . . . .	231
<i>Tobias Pulls</i>	
<b>Author Index</b> . . . . .	247