Audun Jøsang Torleiv Maseng
Svein Johan Knapskog (Eds.)

Identity and Privacy in the Internet Age

14th Nordic Conference on Secure IT Systems, NordSec 2009
Oslo, Norway, 14-16 October 2009
Proceedings

Springer

Volume Editors

Audun Jøsang
University of Oslo
University Graduate Center
Kjeller, Norway
E-mail: josang@unik.no

Torleiv Maseng
Norwegian Defence Research Establishment
Kjeller, Norway
E-mail: Torleiv.Maseng@ffi.no

Svein Johan Knapskog
Norwegian University of Science and Technology
Centre for Quantifiable Quality of Service
in Communication Systems
Trondheim, Norway
E-mail: Knapskog@q2s.ntnu.no

Library of Congress Control Number: 2009935066

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

ISSN 0302-9743
ISBN-10 3-642-04765-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-04765-7 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12769834 06/3180 5 4 3 2 1 0

Preface

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. The 14th Nordic Conference on Secure IT Systems was held in Oslo on 14-16 October 2009. Under the theme Identity and Privacy in the Internet Age, this year's conference explored policies, strategies and technologies for protecting identities and the growing flow of personal information passing through the Internet and mobile networks under an increasingly serious threat picture. Among the contemporary security issues discussed were security services modeling, Petri nets, attack graphs, electronic voting schemes, anonymous payment schemes, mobile ID-protocols, SIM cards, network embedded systems, trust, wireless sensor networks, privacy, privacy disclosure regulations, financial cryptography, PIN verification, temporal access control, random number generators, and some more.

As a pre-cursor to the conference proper, the Nordic Security Day on Wednesday 14 October hosted talks by leading representatives from industry, academia and the government sector, and a press conference was given.

On Thursday 15, a keynote talk was given by Simone Fischer-Hübner, University of Karlstad, Sweden, on the currently strongly researched topic of identity management, entitled *Privacy-Enhancing Identity Management – Challenges for the Future* and on Friday 16 October, a keynote entitled: *Identity Management on the Internet: Opportunities and Challenges for Mobile Operators* was given by Do van Than, Senior Research Scientist at Telenor R&I and Professor at the Norwegian University of Science and Technology (NTNU).

The conference received 52 valid submissions, and 20 regular papers were chosen for presentation and inclusion in the LNCS proceedings by Springer. In addition 8 short papers were chosen for presentation at the conference. All papers were peer reviewed by at least two reviewers, most papers by three, and some by four.

We would like to thank all the people who helped in making the 14th Nordic Conference on Secure IT Systems a scientific and social success. First, we commend the Steering Committee for the decision to allow the conference to be held at the University of Oslo, and for their advice on the general format of the event. Secondly, a heartfelt thanks goes to the Program Committee members and the sub-reviewers who spent valuable time reviewing and discussing the review results. The smooth submission and review processes were run by the Springer OCS, giving invaluable support to the PC, in particular the PC Chair. We also thank the staff at Springer for their advice and support during the preparation of the proceedings.

And last, but not least, we thank the Organizing Committee for the impeccable organization and running of the conference.

October 2009

Audun Jøsang
Torleiv Maseng
Svein Johan Knapskog

Organization

General Chair

Audun Jøsang	University of Oslo – University Graduate Center, Kjeller, Norway

Program Co-chairs

Svein Johan Knapskog	Norwegian University of Science and Technology Center for Quantifiable Quality of Service in Communication Systems, Trondheim, Norway
Torleiv Maseng	Norwegian Defence Research Establishment, Kjeller, Norway University of Lund, Lund, Sweden

Program Committee

Viiveke Fåk	Linköping University, Sweden
Dieter Gollman	University of Technology Hamburg-Harburg, Germany
Peeter Laud	University of Tartu, Estonia
Nahid Shahmehri	Linköping University, Sweden
Simone Fischer-Hübner	Karlstad University, Sweden
Tuomas Aura	Microsoft Research, Cambridge, UK
André Zúquete	University of Aveiro, Portugal
André Årnes	Oracle Norway
Björn Pehrson	KTH – Royal Institute of Technology, Sweden
Chris Mitchell	University of London – Royal Holloway, UK
Christian Damsgaard Jensen	Technical University of Denmark, Denmark
Christian Larsen	National Criminal Investigation Service, Norway
Chunming Rong	University of Stavanger, Norway
Danilo Gligoroski	Norwegian University of Science and Technology, Norway
Denis Trcek	University of Ljubljana, Slovenia
Dogan Kesdogan	University of Siegen, Germany
Ed Dawson	Queensland University of Technology, Australia
Eldfrid Øvstedal	SINTEF, Trondheim, Norway
Eli Winjum	Norwegian Defence Research Establishment, Norway
Erik Hjelmås	Gjøvik University College, Norway

Geir Hallingstad	NATO
George Polyzos	Athens University of Economics and Business, Greece
Inger Anne Tøndel	SINTEF, Trondheim, Norway
Jennifer Seberry	University of Wollongong, Australia
Joakim von Brandis	Mnemonic, Norway
Kåre Presttun	Mnemonic, Norway
Josef Pieprzyk	Macquarie University, Australia
Kai Rannenberg	T-Mobile, Germany
Karin Sallhammar	Telenor, Norway
Knut Johannessen	Telenor, Norway
Lawrie Brown	Australian Defence Force Academy, Australia
Patrick Bours	Gjøvik University College, Norway
Peter Herrmann	Norwegian University of Science and Technology, Norway
Richard Kemmerer	University of California, Santa Barbara, USA
Simin Nadjm-Tehrani	Linköping University, Sweden
Stefan Lindskog	Karlstad University, Sweden
Tomas Olovsson	Chalmers University, Sweden
Tor Helleseth	University of Bergen, Norway
Vlastimil Klima	Independent cryptologist, Czech Republic
Vaclav Matyas	Masaryk University, Czech Republic
Vladimir Oleshchuk	University of Agder, Norway
Wei Wang	INRIA, France
Willy Susilo	University of Wollongong, Australia
Yuliang Zheng	University of North Carolina at Charlotte, USA
Zhili Sun	University of Surrey, UK
Svein Yngvar Willassen	Norwegian University of Science and Technology, Norway
Vijay Varadharajan	Macquarie University, Australia
Mads Dam	Royal Institute of Technology, Sweden
Andrew Clark	Queensland University of Technology, Australia
Anne Karen Seip	The Financial Supervisory Authority of Norway, Norway
Kristian Gjøsteen	Norwegian University of Science and Technology, Norway
Sven Laur	Helsinki University of Technology, Finland
Åsmund Skomedal	Norwegian Computing Center, Norway
Maria Line	SINTEF, Norway

Sponsors

Telenor Group
Nisnet
University of Oslo – University Graduate Center
Norwegian Computing Center

Table of Contents

Session 1: Anonymity and Privacy

Session 2: Modelling and Design

Session 3: Network Layer Security

Session 4: Security for Mobile Users

Session 5: Embedded Systems and Mechanisms

Session 6: Protocols and Protocol Analysis