

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology, Madras, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

More information about this series at <http://www.springer.com/series/7410>

Billy Bob Brumley · Juha Röning (Eds.)

# Secure IT Systems

21st Nordic Conference, NordSec 2016  
Oulu, Finland, November 2–4, 2016  
Proceedings

*Editors*

Billy Bob Brumley  
Tampere University of Technology  
Tampere  
Finland

Juha Röning  
Computer Science and Engineering  
University of Oulu  
Oulu  
Finland

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-47559-2              ISBN 978-3-319-47560-8 (eBook)  
DOI 10.1007/978-3-319-47560-8

Library of Congress Control Number: 2016953314

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer International Publishing AG 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

The NordSec conferences were started in 1996 with the aim of bringing together researchers and practitioners in the field of computer security in the Nordic countries, thereby establishing a forum for discussions and cooperation between universities, industry, and computer societies. 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.

These proceedings contain the papers presented at NordSec 2016: the 21st Nordic Conference on Secure IT Systems held during November 2–4, 2016, in Oulu, Finland. The venue was the University of Oulu, co-located with the 10th International Crisis Management Workshop and Oulu Winter School.

Of the 49 total submissions received by the July 8 extended deadline, 43 met the requirements for peer review. After a brief manuscript bidding process, the review period spanned July 12 through August 10, during which the 29-member Program Committee along with 20 external reviewers produced a total of 151 reviews. With an average of 3.5 reviews per manuscript, this strong effort brought us quite close to our goal of four reviews per manuscript.

Based on the reviews and following a brief yet active discussion phase, we notified authors on August 15 that 16 manuscripts were accepted for presentation at NordSec 2016. Amongst these papers, five clear themes emerged: system security, network security, software security, cryptography, and authentication. Furthermore, the accepted papers suggest cyber-physical system security is currently an active academic research area.

We were honored to have three brilliant invited speakers: (1) Shay Gueron, University of Haifa, Israel, and Intel Corporation (Intel Development Center, Haifa, Israel); (2) Jan-Erik Ekberg (Trustonic); (3) Daniel Komaromy (Comsecuris).

As NordSec 2016 chairs, we extend our sincerest gratitude to everyone involved in making this year's instance a success, including but not limited to: the authors who submitted their hard work, the Program Committee and external reviewers, the invited speakers, Christian Wieser (Conference Ops), and our generous sponsors Ericsson and Intopalo.

September 2016

Billy Bob Brumley  
Juha Rönning

# Organization

## General Chair

Juha Röning                      University of Oulu, Finland

## Program Chair

Billy Bob Brumley              Tampere University of Technology, Finland

## Conference Operations

Christian Wieser                University of Oulu, Finland

## Program Committee

Magnus Almgren	Chalmers University of Technology, Sweden
David Bernhard	University of Bristol, UK
Billy Bob Brumley	Tampere University of Technology, Finland
Mads Dam	KTH Royal Institute of Technology, Sweden
Nicola Dragoni	Technical University of Denmark, Denmark
Danilo Gligoroski	Norwegian University of Science and Technology, Norway
Eric Xu Guo	Qualcomm, USA
Kimmo Halunen	VTT Technical Research Centre of Finland, Finland
Chris Hankin	Imperial College London, UK
Rene Rydhof Hansen	Aalborg University, Denmark
Daniel Hedin	Mälardalen University, Sweden
Marko Helenius	Tampere University of Technology, Finland
Kimmo Järvinen	Aalto University, Finland
Frank Kargl	Ulm University, Germany
Svein Johan Knapskog	Norwegian University of Science and Technology, Norway
Hanno Langweg	Norwegian University of Science and Technology, Norway
Peeter Laud	Cybernetica AS, Estonia
Samuel Marchal	Aalto University, Finland
Fabio Martinelli	IIT-CNR, Italy
Chris Mitchell	Royal Holloway, University of London, UK
Hanne Riis Nielson	Technical University of Denmark, Denmark
Valtteri Niemi	University of Helsinki, Finland
Andrew Paverd	Aalto University, Finland

Kai Rannenberg  
Heiko Roßnagel  
Juha Rönning  
Ben Smeets  
Seppo Virtanen  
Xueyang Wang

Goethe University Frankfurt, Germany  
Fraunhofer IAO, Germany  
University of Oulu, Finland  
Lund University, Sweden  
University of Turku, Finland  
Intel, USA

## **Additional Reviewers**

Fatma Al Maqbali  
Zaruhi Aslanyan  
Fabina Dietrich  
Per Hallgren  
Daniel Hausknecht  
Kekai Hu  
Sebastian Kurowski

Hugo A. López  
John Mattsson  
Flemming Nielson  
Andrea Saracino  
T. Schafeitel-Tähtinen  
Christopher Schmitz  
Alexander Sjösten

Angelo Spognardi  
Fatbardh Veseli  
Luca Viganò  
Shuzhe Yang  
Artsiom Yautsiukhin  
Ahmed Seid Yesuf

## **Sponsors**

Ericsson  
Intopalo



**ERICSSON**



# Contents

## System Security

Event-Triggered Watermarking Control to Handle Cyber-Physical Integrity Attacks . . . . .	3
<i>Jose Rubio-Hernan, Luca De Cicco, and Joaquin Garcia-Alfaro</i>	
Detecting Process-Aware Attacks in Sequential Control Systems. . . . .	20
<i>Oualid Koucham, Stéphane Mocanu, Guillaume Hiet, Jean-Marc Thiriet, and Frédéric Majorczyk</i>	
Towards an Automated and Dynamic Risk Management Response System. . .	37
<i>Gustavo Gonzalez-Granadillo, Ender Alvarez, Alexander Motzek, Matteo Merialdo, Joaquin Garcia-Alfaro, and Hervé Debar</i>	
Understanding How Components of Organisations Contribute to Attacks . . .	54
<i>Min Gu, Zaruhi Aslanyan, and Christian W. Probst</i>	
A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks . . . . .	67
<i>Sandra König, Stefan Schauer, and Stefan Rass</i>	

## Network Security

Creating and Detecting IPv6 Transition Mechanism-Based Information Exfiltration Covert Channels. . . . .	85
<i>Bernhards Blumbergs, Mauno Pihelgas, Markus Kont, Olaf Maennel, and Risto Vaarandi</i>	
ML: DDoS Damage Control with MPLS . . . . .	101
<i>Pierre-Edouard Fabre, Hervé Debar, Jouni Viinikka, and Gregory Blanc</i>	

## Software Security

Empirical Analysis on the Use of Dynamic Code Updates in Android and Its Security Implications. . . . .	119
<i>Maqsood Ahmad, Bruno Crispo, and Teklay Gebremichael</i>	
Evaluation of Resource-Based App Repackaging Detection in Android . . . . .	135
<i>Olga Gadyatskaya, Andra-Lidia Lezza, and Yuri Zhauniarovich</i>	



A Survey on Internal Interfaces Used by Exploits and Implications on  
Interface Diversification . . . . . 152  
*Sampsa Rauti, Samuel Lauren, Joni Uitto, Shohreh Hosseinzadeh,  
Jukka Ruohonen, Sami Hyrynsalmi, and Ville Leppänen*

A Tale of the OpenSSL State Machine: A Large-Scale Black-Box Analysis . . . 169  
*Joeri de Ruiter*

**Cryptography**

Speeding up R-LWE Post-quantum Key Exchange . . . . . 187  
*Shay Gueron and Fabian Schlieker*

Efficient Sparse Merkle Trees: Caching Strategies and Secure (Non-)  
Membership Proofs . . . . . 199  
*Rasmus Dahlberg, Tobias Pulls, and Roel Peeters*

Secure Multiparty Sorting Protocols with Covert Privacy . . . . . 216  
*Peeter Laud and Martin Pettai*

**Authentication**

PASSPHONE: Outsourcing Phone-Based Web Authentication While  
Protecting User Privacy . . . . . 235  
*Martin Potthast, Christian Forler, Eik List, and Stefan Lucks*

Secure, Usable and Privacy-Friendly User Authentication from Keystroke  
Dynamics. . . . . 256  
*Kimmo Halunen and Visa Vallivaara*

**Author Index** . . . . . 269