

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA


Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung 

Columbia University, New York, NY, USA


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


Nicola Taveri · Antonis Michalas ·
Billy Bob Brumley (Eds.)


Secure IT Systems

26th Nordic Conference, NordSec 2021
Virtual Event, November 29–30, 2021
Proceedings

Editors

Nicola Tuveri 
Tampere University
Tampere, Finland

Antonis Michalas 
Tampere University
Tampere, Finland

Billy Bob Brumley 
Tampere University
Tampere, Finland

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-91624-4 ISBN 978-3-030-91625-1 (eBook)
<https://doi.org/10.1007/978-3-030-91625-1>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2021

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, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland 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 within 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 2021: The 26th Nordic Conference on Secure IT Systems held virtually, due to COVID-19 restrictions, during November 29–30, 2021. The conference was organized by the [Network and Information Security \(NISEC\)](#) group at Tampere University, Finland.

All of the 29 submissions received by the extended deadline (August 31), met the requirements for peer review. Following a brief bidding process for manuscripts, the review period was set between September 8 and September 27. During this period the 45-member Program Committee produced a total of 111 reviews. The average of 3.83 reviews per manuscript achieved by this well-organized effort brought us close to our initial goal of 4 reviews per manuscript.

Based on the reviews and following a brief yet active discussion phase, we notified authors on October 1 that 11 manuscripts had been accepted for presentation at NordSec 2021, resulting in a 37.93% acceptance rate. Amongst these papers, five clear themes emerged: applied cryptography, security in Internet of Things, machine learning and security, network security, and trust.

We were honored to have two brilliant invited speakers: [David Arroyo](#) from ITEFI-CSIC, Spain, and [Rafael Dowsley](#) from Monash University, Australia.

As NordSec 2021 chairs, we extend our sincerest gratitude to everyone involved in making this year's event a success, including but not limited to the authors that submitted their hard work, the Program Committee and external reviewers, and the invited speakers.

October 2021

Billy Bob Brumley
Antonis Michalas
Nicola Taveri

Organization

General Chair

Billy Bob Brumley Tampere University, Finland

Program Chair

Antonis Michalas Tampere University, Finland

Local Chair

Nicola Taveri Tampere University, Finland

Steering Committee

Magnus Almgren	Chalmers University of Technology, Sweden
Tuomas Aura	Aalto University, Finland
Karin Bernsmed	SINTEF ICT and Norwegian University of Science and Technology, Norway
Billy Bob Brumley	Tampere University, Finland
Sonja Buchegger	KTH Royal Institute of Technology, Sweden
Bengt Carlsson	Blekinge Institute of Technology, Sweden
Úlfar Erlingsson	Google Inc., Mountain View, USA
Simone Fischer-Huebner	Karlstad University, Sweden
Dieter Gollmann	Hamburg University of Technology, Germany
Nils Gruschka	University of Oslo, Norway
Audun Jøsang	University of Oslo, Norway
Stewart Kowalski	Norwegian University of Science and Technology, Norway
Peeter Laud	Cybernetica AS, Estonia
Helger Lipmaa	University of Tartu, Estonia
Katerina Mitrokotsa	Chalmers University of Technology, Sweden
Simin Nadjm-Tehrani	Linköping University, Sweden
Hanne Riis Nielson	Technical University of Denmark, Denmark
Juha Rönning	University of Oulu, Finland
Andrei Sabelfeld	Chalmers University of Technology, Sweden

Program Committee

Magnus Almgren	Chalmers University of Technology, Sweden
Mikael Asplund	Linköping University, Sweden
Stefan Axelsson	Stockholm University, Sweden
Musard Balliu	KTH Royal Institute of Technology, Sweden
Felipe Boeira	Linköping University, Sweden
Sonja Buchegger	KTH Royal Institute of Technology, Sweden
Hai-Van Dang	Plymouth University, UK
Tassos Dimitriou	Computer Technology Institute, Greece, and Kuwait University, Kuwait
Nicola Dragoni	Technical University of Denmark, Denmark
György Dán	KTH Royal Institute of Technology, Sweden
Mathias Ekstedt	KTH Royal Institute of Technology, Sweden
Ulrik Franke	RISE, Sweden
Christian Gehrman	Lund University, Sweden
Kristian Gjølsteen	Norwegian University of Science and Technology, Norway
Dieter Gollmann	Hamburg University of Technology, Germany
Nils Gruschka	University of Oslo, Norway
Mohammad Hamad	Technical University of Munich, Germany
Rene Rydhof Hansen	Aalborg University, Denmark
Tor Hellese	University of Bergen, Norway
Martin Gilje Jaatun	SINTEF Digital, Norway
Meiko Jensen	Kiel University of Applied Sciences, Germany
Thomas Johansson	Lund University, Sweden
Audun Josang	University of Oslo, Norway
Ulf Kargén	Linköping University, Sweden
Mohsin Khan	University of Helsinki, Finland
Marcel Kyas	Reykjavík University, Iceland
Ville Leppänen	University of Turku, Finland
Stefan Lindskog	Karlstad University, Sweden
Olaf Maennel	Tallinn University of Technology, Estonia
Raimundas Matulevicius	University of Tartu, Estonia
Per Håkon Meland	SINTEF ICT, Norway
Simin Nadjm-Tehrani	Linköping University, Sweden
Nils Nordbotten	Thales Norway and University of Oslo, Norway
Tomas Olovsson	Chalmers University of Technology, Sweden
Nicolae Paladi	Lund University and CanaryBit AB, Sweden
Arnis Paršovs	University of Tartu, Estonia
Shahid Raza	RISE SICS, Sweden
Hans P. Reiser	University of Passau, Germany
Juha Röning	University of Oulu, Finland
Einar Snekkenes	Norwegian University of Science and Technology, Norway
Emmanouil Vasilomanolakis	Aalborg University, Denmark
Øyvind Ytrehus	University of Bergen, Norway

Additional Reviewers

David Arroyo

Mariia Bakhtina

Anton Christensen

Ignacio Delgado-Lozano

Iaroslav Gridin

Mubashar Iqbal

Johannes Köstler

Cesar Pereida García

Henrich C. Pöhls

Mari Seeba

Stefan Varga

Contents

Applied Cryptography

Communicating Through Subliminal-Free Signatures	3
<i>George Teşeleanu</i>	
Size, Speed, and Security: An Ed25519 Case Study	16
<i>Cesar Pereida García and Sampo Sovio</i>	
Arrows in a Quiver: A Secure Certificateless Group Key Distribution Protocol for Drones	31
<i>Eugene Frimpong, Reyhaneh Rabbaninejad, and Antonis Michalas</i>	

Security in Internet of Things

X-Pro: Distributed XDP Proxies Against Botnets of Things	51
<i>Syafiq Al Atiiq and Christian Gehrman</i>	
Industrialising Blackmail: Privacy Invasion Based IoT Ransomware	72
<i>Calvin Brierley, Budi Arief, David Barnes, and Julio Hernandez-Castro</i>	

Machine Learning and Security

SQL Injections and Reinforcement Learning: An Empirical Evaluation of the Role of Action Structure	95
<i>Manuel Del Verme, Åvald Åslaugson Sommervoll, László Erdődi, Simone Totaro, and Fabio Massimo Zennaro</i>	
Secure Collaborative Learning for Predictive Maintenance in Optical Networks	114
<i>Khouloud Abdelli, Joo Yeon Cho, and Stephan Pachnicke</i>	

Network Security

Collector: Measuring Domain Name Dark Matter from Different Vantage Points	133
<i>Kaspar Hageman, René Rydhof Hansen, and Jens Myrup Pedersen</i>	
Adversarial Trends in Mobile Communication Systems: From Attack Patterns to Potential Defenses Strategies	153
<i>Hsin Yi Chen and Siddharth Prakash Rao</i>	

Trust

Trusted Sockets Layer: A TLS 1.3 Based Trusted Channel Protocol 175
Arto Niemi, Vasile Adrian Bogdan Pop, and Jan-Erik Ekberg

Preliminary Security Analysis, Formalisation, and Verification
of OpenTitan Secure Boot Code 192
*Bjarke Hilmer Møller, Jacob Gosch Søndergaard,
Kristoffer Skagbæk Jensen, Magnus Winkel Pedersen,
Tobias Worm Bøgedal, Anton Christensen, Danny Bøgsted Poulsen,
Kim Guldstrand Larsen, René Rydhof Hansen, Thomas Rosted Jensen,
Heino Juvoll Madsen, and Henrik Uhrenfeldt*

Author Index 213