

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, Chennai, 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>

Nils Gruschka (Ed.)

Secure IT Systems

23rd Nordic Conference, NordSec 2018
Oslo, Norway, November 28–30, 2018
Proceedings

Editor
Nils Gruschka 
University of Oslo
Oslo, Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-03637-9 ISBN 978-3-030-03638-6 (eBook)
<https://doi.org/10.1007/978-3-030-03638-6>

Library of Congress Control Number: 2018960426

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2018

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. 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

This volume contains the papers presented at NordSec 2018, the 23rd Nordic Conference on Secure IT Systems. The conference was held during November 28–30, 2018, in Oslo, Norway.

The NordSec conferences started in 1996 with the aim of bringing together researchers and practitioners in computer security in the Nordic countries, thereby establishing a forum for discussion and cooperation between universities, industry, and computer societies. NordSec addresses a broad range of topics within IT security and privacy and over the years it has developed into an international conference that takes place in the Nordic countries. NordSec is currently a key meeting venue for Nordic university teachers and students with research interests in information security and privacy.

NordSec 2018 received 81 submissions of full research papers, with all valid submissions receiving three double-blinded reviews by the Program Committee (PC). After the reviewing phase, 29 papers were accepted for publication and are included in these proceedings. Furthermore, we organized a poster session that encouraged discussion and brainstorming on current topics of information security and privacy.

We were honored to host three brilliant invited speakers presenting talks on current topics in information security focusing on cybersecurity and privacy. More precisely, Dr. Martin Eian from mnemonic gave a talk on “Cybersecurity Threats to the Academic Sector,” Dr. Lothar Fritsch from Karlstad University gave a talk on “From Risk to Treatment: Privacy Impact Assessment and Privacy Controls,” and Prof. Christoph Sorge from Saarland University gave a talk on “Smart Meter Privacy: An Interdisciplinary Perspective.”

We sincerely thank everyone involved in making this year’s instance a success, including, but not limited to: the authors who submitted their papers, the presenters who contributed to the NordSec program, and the PC members and additional reviewers for their thorough and very helpful reviews.

November 2018

Nils Gruschka

Organization

Conference Chairs

General Chair

Audun Jøsang University of Oslo, Norway

Program Chair

Nils Gruschka University of Oslo, Norway

Publicity Chair

Kamer Vishi University of Oslo, Norway

Poster Chair

Mathias Ekstedt Royal Institute of Technology, Sweden

Program Committee

Magnus Almgren	Chalmers University of Technology, Sweden
Hamed Arshad	University of Oslo, Norway
Mikael Asplund	Linköping University, Sweden
Musard Balliu	KTH Royal Institute of Technology, Sweden
Patrick Bours	Norwegian University of Science and Technology, Norway
Colin Boyd	Norwegian University of Science and Technology, Norway
Siri Bromander	mnemonic as, Norway
Billy Brumley	Tampere University of Technology, Finland
Sonja Buchegger	KTH Royal Institute of Technology, Sweden
Ahto Buldas	Tallinn University of Technology, Estonia
György Dán	KTH Royal Institute of Technology, Sweden
Martin Eian	mnemonic, Norway
Laszlo Erdodi	University of Oslo, Norway
Daniel Fava	University of Oslo, Norway
Simone Fischer-Hübner	Karlstad University, Sweden
Ulrik Franke	Swedish Institute of Computer Science, Sweden
Lothar Fritsch	Karlstad University, Sweden
Kristian Gjøsteen	Norwegian University of Science and Technology, Norway
Jonas Hallberg	Swedish Defence Research Agency, Sweden
Rene Rydhof Hansen	Aalborg University, Denmark

Tore Helleseth	University of Bergen, Norway
Martin Gilje Jaatun	SINTEF Digital, Norway
Justinas Janulevicius	VG TU, Lithuania
Meiko Jensen	Syddansk Universitet, Denmark
Thomas Johansson	Lund University, Sweden
Pontus Johnson	KTH Royal Institute of Technology, Sweden
Sokratis Katsikas	Norwegian University of Science and Technology, Norway
Stewart James Kowalski	Norwegian University of Science and Technology, Norway
Martti Lehto	University of Jyväskylä, Finland
Ville Leppänen	University of Turku, Finland
Luigi Lo Iacono	Technical University of Cologne, Germany
Ijlal Loutfi	University of Oslo, Norway
Henning Maagerud	Norges forskningsråd, Norway
Olaf Maennel	Tallinn University of Technology, Estonia
Tobias Mahler	University of Oslo, Norway
Raimundas Matulevicius	University of Tartu, Estonia
Vasileios Mavroeidis	University of Oslo, Norway
Aikaterini Mitrokotsa	Chalmers University of Technology, Sweden
Simin Nadjm-Tehrani	Linköping University, Sweden
Nils Nordbotten	FFI, Norway
Christian W. Probst	Unitec Institute of Technology, New Zealand
Carla Ràfols	Pompeu Fabra University, Spain
Shahid Raza	RISE SICS Stockholm, Sweden
Juha Röning	University of Oulu, Finland
Lillian Røstad	Sopra Steria, Norway
Alejandro Russo	Chalmers University of Technology, Sweden
Berry Schoenmakers	Eindhoven University of Technology, The Netherlands
Carsten Schuermann	IT University of Copenhagen, Denmark
Einar Snekkenes	Norwegian University of Science and Technology, Norway
Åvald Sommervoll	University of Oslo, Norway
Shukun Tokas	University of Oslo, Norway
Alexandre Vernotte	KTH Royal Institute of Technology, Sweden
Øyvind Ytrehus	University of Bergen, Norway
Fabio Zennaro	University of Oslo, Norway
Bingsheng Zhang	Lancaster University, UK

Additional Reviewers

A. C. Aldaya
M. Algehed
N. J. Bouman
C. Brunetta
A. Bruni
A. Cretin
P. Davis
M. K. Farmad
C. P. García
R. Giustolisi
B. Liang

F. Mancini
O. Mir
M. Mollaefar
N. Momen
S. Petrovic
A. Sharif
E. Shereen
J. Tom
L. Tosoni
A. Tossou
M. Vassena

Contents

Privacy

Privacy-Preserving Distributed Economic Dispatch Protocol for Smart Grid	3
<i>Avikarsha Mandal, Frederik Armknecht, and Erik Zenner</i>	
Tracking Information Flow via Delayed Output: Addressing Privacy in IoT and Emailing Apps	19
<i>Iulia Bastys, Frank Piessens, and Andrei Sabelfeld</i>	
MixMesh Zones – Changing Pseudonyms Using Device-to-Device Communication in Mix Zones	38
<i>Mirja Nitschke, Philipp Holler, Lukas Hartmann, and Doğan Kesdoğan</i>	
AppLance: A Lightweight Approach to Detect Privacy Leak for Packed Applications	54
<i>Hongliang Liang, Yudong Wang, Tianqi Yang, and Yue Yu</i>	

Cryptography

Unifying Kleptographic Attacks	73
<i>George Teşeleanu</i>	
Steady: A Simple End-to-End Secure Logging System.	88
<i>Tobias Pulls and Rasmus Dahlberg</i>	
Revisiting Deniability in Quantum Key Exchange: via Covert Communication and Entanglement Distillation	104
<i>Arash Atashpendar, G. Vamsi Policharla, Peter B. Rønne, and Peter Y. A. Ryan</i>	
On Security Analysis of Generic Dynamic Authenticated Group Key Exchange	121
<i>Zheng Yang, Mohsin Khan, Wanping Liu, and Jun He</i>	
A Blockchain-Assisted Hash-Based Signature Scheme	138
<i>Ahto Buldas, Risto Laanoja, and Ahto Truu</i>	
The Fiat-Shamir Zoo: Relating the Security of Different Signature Variants.	154
<i>Matilda Backendal, Mihir Bellare, Jessica Sorrell, and Jiahao Sun</i>	

Verifiable Light-Weight Monitoring for Certificate Transparency Logs	171
<i>Rasmus Dahlberg and Tobias Pulls</i>	

Network and Cloud Security

<i>CLort</i> : High Throughput and Low Energy Network Intrusion Detection on IoT Devices with Embedded GPUs.	187
<i>Charalampos Stylianopoulos, Linus Johansson, Oskar Olsson, and Magnus Almgren</i>	

Detection of Covert Channels in TCP Retransmissions	203
<i>Sebastian Zillien and Steffen Wendzel</i>	

What You Can Change and What You Can't: Human Experience in Computer Network Defenses	219
<i>Vivien M. Rooney and Simon N. Foley</i>	

Attack Simulation for a Realistic Evaluation and Comparison of Network Security Techniques	236
<i>Alexander Bajic and Georg T. Becker</i>	

<i>Sarracenia</i> : Enhancing the Performance and Stealthiness of SSH Honeypots Using Virtual Machine Introspection	255
<i>Stewart Sentanoe, Benjamin Taubmann, and Hans P. Reiser</i>	

Authorization Policies Specification and Consistency Management within Multi-cloud Environments	272
<i>Ehtesham Zahoor, Asim Ikram, Sabina Akhtar, and Olivier Perrin</i>	

Cyber Security and Malware

Cyber Hygiene: The Big Picture	291
<i>Kaie Maennel, Sten Mäses, and Olaf Maennel</i>	

Estimating the Risk of Fraud Against E-Services.	306
<i>Ahmed Seid Yesuf and Christian W. Probst</i>	

PESTEL Analysis of Hacktivism Campaign Motivations	323
<i>Juha Nurmi and Mikko S. Niemelä</i>	

Data Modelling for Predicting Exploits	336
<i>Alexander Reinthal, Eleftherios Lef Filippakis, and Magnus Almgren</i>	

UpDroid: Updated Android Malware and Its Familial Classification	352
<i>Kursat Aktas and Sevil Sen</i>	

Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework	369
<i>Barbara Krumay, Edward W. N. Bernroider, and Roman Walser</i>	
Next Generation Cryptographic Ransomware	385
<i>Ziya Alper Genç, Gabriele Lenzini, and Peter Y. A. Ryan</i>	
Security for Software and Software Development	
Hardware-Assisted Program Execution Integrity: HAPEI	405
<i>Ronan Lashermes, Hélène Le Boudier, and Gaël Thomas</i>	
Protecting Instruction Set Randomization from Code Reuse Attacks	421
<i>Roberto Guanciale</i>	
A Uniform Information-Flow Security Benchmark Suite for Source Code and Bytecode	437
<i>Tobias Hamann, Mihai Herda, Heiko Mantel, Martin Mohr, David Schneider, and Markus Tasch</i>	
When Harry Met Tinder: Security Analysis of Dating Apps on Android	454
<i>Kuyju Kim, Taeyun Kim, Seungjin Lee, Soolin Kim, and Hyounghick Kim</i>	
Threat Poker: Solving Security and Privacy Threats in Agile Software Development.	468
<i>Hanne Rygge and Audun Jøsang</i>	
Author Index	485