

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>


Thyla van der Merwe · Chris Mitchell ·
Maryam Mehrnezhad (Eds.)


Security Standardisation Research

6th International Conference, SSR 2020
London, UK, November 30 – December 1, 2020
Proceedings

Editors

Thyla van der Merwe 
Mozilla
London, UK

Maryam Mehrnezhad 
School of Computing
Newcastle University
Newcastle upon Tyne, UK

Chris Mitchell 
Information Security Department
Royal Holloway, University of London
Egham, UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-64356-0 ISBN 978-3-030-64357-7 (eBook)
<https://doi.org/10.1007/978-3-030-64357-7>

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2020

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 6th Conference on Security Standardisation Research (SSR 2020) was held as an online conference during November 30 – December 1, 2020. The main purpose of this conference was to discuss the many research problems deriving from studies of existing standards, the development of revisions to existing standards, and the exploration of completely new areas of standardization. Additionally, as in previous years, SSR 2020 aimed to be a platform for exchanging knowledge between academia and industry, with the goal of improving the security of standardized systems.

Overall, there were 20 submissions to SSR 2020, of which 7 were accepted. Apart from a couple of papers rejected because they did not obey the submission instructions, all submissions were reviewed by at least three Program Committee members. The accepted papers cover a range of topics in the field of security standardization research, including analysis, evaluation, and comparison of standards and their implementations, standards development, improving existing standards, and potential future areas of standardization.

As an innovation, this year we encouraged submissions in the area of legal aspects of data protection and privacy. The focus on privacy was reflected in a number of our submissions and accepted papers. In addition to regular research papers, we also encouraged the submission of Systematization of Knowledge (SoK) papers relating to security standardization as well as Vision papers. The vision track was intended to report on work in progress or concrete ideas for work that has yet to begin. The diversity in types of submissions was well received by the authors. The set of accepted papers is made up of five research papers, one SoK paper, and one vision paper.

The SSR 2020 program included two invited keynote addresses to shed light on security standardization from both industrial and academic perspectives.

- Professor Ligu Chen, University of Surrey, UK
- Nick Sullivan, Cloudflare, USA

We would like to thank all the people who contributed to the success of SSR 2020. First, we thank the authors for submitting their work to our conference. We heartily thank the Program Committee for their careful and thorough reviews. Thanks must also go to the shepherds for their expert guidance and helpful advice on improving papers. We are grateful to all the people at Mozilla, who supported hosting SSR 2020 as a virtual conference. Finally, we thank all the attendees of SSR 2020.

October 2020

Maryam Mehrnezhad
Thyla van der Merwe
Chris Mitchell

Gaëtan Pradel	INCERT, Luxembourg
Raphael Spreitzer	SGS Digital Trust Services GmbH, Austria
Ehsan Toreini	Durham University, UK
Christopher Wood	Cloudflare, USA
Joanne Woodage	Microsoft Research Cambridge, UK
Kazuki Yoneyama	Ibaraki University, Japan

External Reviewers

Dustin Moody	NIST, USA
Ray Perlner	NIST, USA

Contents

On the Memory Fault Resilience of TLS 1.3	1
<i>Lukas Brandstetter, Marc Fischlin, Robin Leander Schröder, and Michael Yonli</i>	
On Internal Re-keying	23
<i>Liliya Akhmetzyanova, Evgeny Alekseev, Stanislav Smyshlyaev, and Igor Oshkin</i>	
A Systematic Appraisal of Side Channel Evaluation Strategies	46
<i>Melissa Azouaoui, Davide Bellizia, Ileana Buhan, Nicolas Debande, Sébastien Duval, Christophe Giraud, Èliane Jaulmes, François Koeune, Elisabeth Oswald, François-Xavier Standaert, and Carolyn Whitnall</i>	
Taming the Many EdDSAs	67
<i>Konstantinos Chalkias, François Garillot, and Valeria Nikolaenko</i>	
SoK: Comparison of the Security of Real World RSA Hash-and-Sign Signatures.	91
<i>Saqib A. Kakvi</i>	
The Vacuity of the Open Source Security Testing Methodology Manual	114
<i>Martin R. Albrecht and Rikke Bjerg Jensen</i>	
Vision: A Critique of Immunity Passports and W3C Decentralized Identifiers.	148
<i>Harry Halpin</i>	
Author Index	169