

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>


Robert Krimmer · Melanie Volkamer
Véronique Cortier · Rajeev Goré
Manik Hapsara · Uwe Serdült
David Duenas-Cid (Eds.)

Electronic Voting

Third International Joint Conference, E-Vote-ID 2018
Bregenz, Austria, October 2–5, 2018
Proceedings


Editors


Robert Krimmer 
Tallinn University of Technology
Tallinn
Estonia

Melanie Volkamer 
Karlsruhe Institute of Technology
Karlsruhe
Germany

Véronique Cortier
LORIA
Vandoeuvre-lès-Nancy Cedex
France

Rajeev Goré
Australian National University
Canberra, ACT
Australia

Manik Hapsara 
University of New South Wales
Canberra, ACT
Australia

Uwe Serdült 
Ritsumeikan University
Kusatsu, Shiga
Japan

David Duenas-Cid 
Tallinn University of Technology
Tallinn
Estonia

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-00418-7 ISBN 978-3-030-00419-4 (eBook)
<https://doi.org/10.1007/978-3-030-00419-4>

Library of Congress Control Number: 2018953823

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 papers presented at E-Vote-ID 2018, the Third International Joint Conference on Electronic Voting, held during October 2–5, 2018, in Bregenz, Austria. It resulted from the merging of EVOTE and Vote-ID.

In total, more than 800 experts from over 35 countries have attended the conference series over the last 14 years. This shows that the conference continues to be one of the major events in the field of electronic voting, providing ample room for interdisciplinary and open discussion of all issues relating to electronic voting.

Also, this year, the conference consisted of:

- Security, Usability and Technical Issues Track
- Administrative, Legal, Political and Social Issues Track
- Election and Practical Experiences Track
- PhD Colloquium on the day before the conference

This year's edition, E-VOTE-ID 2018, received 45 submissions, being, each of them, reviewed by 3 to 4 program committee members, using a double blind-review process. As a result, 13 papers were accepted for this volume, representing 29% of the submitted proposals. The selected papers cover a wide range of topics connected with electronic voting, including experiences and revisions of the real uses of E-voting systems and corresponding processes in elections.

Special thanks go to the members of the international program committee for their hard work in reviewing, discussing, and shepherding papers. They ensured the high quality of these proceedings with their knowledge and experience. We would also like to thank the German Informatics Society (Gesellschaft für Informatik) with its ECOM working group for their partnership over many years.

October 2018

Robert Krimmer
Melanie Volkamer
Véronique Cortier
Rajeev Goré
Manik Hapsara
Uwe Serdült
David Duenas-Cid

Organization

Program Committee

Myrto Arapinis	The University of Edinburgh, UK
Roberto Araujo	Universidade Federal do Pará, Brazil
Jordi Barrat i Esteve	eVoting Legal Lab, Catalonia
Josh Benaloh	Microsoft, USA
David Bismark	Votato, Sweden
Nadja Braun Binder	University of Zurich, Switzerland
Christian Bull	The Norwegian Ministry of Local Government and Regional Development, Norway
Susanne Caarls	Election Consultant, Netherlands
Gianpiero Catozzi	UNDP, USA
Véronique Cortier	CNRS, Loria, France
Stephanie Delaune	IRISA, France
Ardita Driza Maurer	Zentrum für Demokratie Aarau and Zurich University, Switzerland
David Duenas-Cid	Tallinn University of Technology, Estonia
Aleksander Essex	University of Western Ontario, Canada
Joshua Franklin	NIST, USA
David Galindo	University of Birmingham, UK
Micha Germann	Katholieke Universiteit Leuven, Belgium
J. Paul Gibson	Mines-Télécom, France
Kristian Gjosteen	Norwegian University of Science and Technology, Norway
Nicole Goodman	University of Toronto, Canada
Rajeev Goré	Australian National University, Australia
Ruediger Grimm	University of Koblenz, Germany
Rolf Haenni	Bern University of Applied Sciences, Switzerland
Thomas Haines	Queensland University of Technology, Australia
Thad Hall	MPR, USA
Manik Hapsara	The University of New South Wales, Australia
Toby James	University of East Anglia, UK
Tarmo Kalvet	Ragnar Nurkse School of Innovation and Governance at Tallinn University of Technology, Estonia
Norbert Kersting	University of Münster, Germany
Aggelos Kiayias	National and Kapodistrian University Athens, Greece
Shin Kim	Hallym University, South Korea
Reto Koenig	Bern University of Applied Sciences, Switzerland
Robert Krimmer	Ragnar Nurkse School of Innovation and Governance at Tallinn University of Technology, Estonia

Ralf Kuesters	University of Stuttgart, Germany
Oksana Kulyk	TU Darmstadt, Germany
Dan Malinovich	UNDP, USA
Steven Martin	OSCE/ODIHR, Poland
Anu Masso	ETH Zurich, Switzerland
Ronan McDermott	Independent Election Expert, Switzerland
Juan Manuel Mecinas	Centro de Investigación y Docencia Económica, Mexico
Hannu Nurmi	University of Turku, Finland
Jon Pammett	Carleton University, Canada
Olivier Pereira	Universite catholique de Louvain, Belgium
Goran Petrov	Independent Election Expert, Macedonia
Marco Prandini	Università di Bologna, Italy
Josep M ^a Reniu	University of Barcelona, Spain
Peter Roenne	SnT, University of Luxembourg, Luxembourg
Mark Ryan	University of Birmingham, UK
P. Y. A. Ryan	University of Luxembourg, Luxembourg
Steve Schneider	University of Surrey, UK
Berry Schoenmakers	Eindhoven University of Technology, The Netherlands
Carsten Schuermann	IT University of Copenhagen, Denmark
Uwe Serdült	University of Zurich, Switzerland
Vanessa Teague	Melbourne School of Engineering, Australia
Tomasz Truderung	Polyas, Germany
Priit Vinkel	State Electoral Office of Estonia, Estonia
Melanie Volkamer	Karlsruhe Institute of Technology, Germany
Kåre Vollan	Quality AS, Norway
Bogdan Warinschi	University of Bristol, UK
Roland Wen	The University of New South Wales, Australia
Gregor Wenda	BMI, Austria
Peter Wolf	International IDEA, Sweden
Michael Yard	IFES, Lybia
Filip Zagorski	Wroclaw University of Technology, Poland

Contents

Computing the Margin of Victory in Preferential Parliamentary Elections. . . .	1
<i>Michelle Blom, Peter J. Stuckey, and Vanessa J. Teague</i>	
Ballot-Polling Risk Limiting Audits for IRV Elections.	17
<i>Michelle Blom, Peter J. Stuckey, and Vanessa J. Teague</i>	
The Threat of SSL/TLS Stripping to Online Voting.	35
<i>Anthony Cardillo and Aleksander Essex</i>	
Modular Formalisation and Verification of STV Algorithms.	51
<i>Milad K. Ghale, Rajeev Goré, Dirk Pattinson, and Mukesh Tiwari</i>	
Online Voting in Indigenous Communities: Lessons from Canada.	67
<i>Nicole Goodman, Chelsea Gabel, and Brian Budd</i>	
Process Models for Universally Verifiable Elections	84
<i>Rolf Haenni, Eric Dubuis, Reto E. Koenig, and Philipp Locher</i>	
Model Checking the SELENE E-Voting Protocol in Multi-agent Logics	100
<i>Wojciech Jamroga, Michal Knapik, and Damian Kurpiewski</i>	
How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia	117
<i>Robert Krimmer, David Duenas-Cid, Iuliia Krivonosova, Priit Vinkel, and Arne Koitmaa</i>	
Implementing an Audio Side Channel for Paper Voting.	132
<i>Kristjan Krips, Jan Willemson, and Sebastian Värv</i>	
The E-voting Readiness Index and the Netherlands	146
<i>Leontine Loeber</i>	
Winning the Election, but Losing the Litigation: A Prognosis of Nigerian Judicial Attitudes Toward Evidence Produced from ‘E-Accreditation Machines’.	160
<i>Felix Oludare Omosole</i>	
Risk-Limiting Audits by Stratified Union-Intersection Tests of Elections (SUITE).	174
<i>Kellie Ottoboni, Philip B. Stark, Mark Lindeman, and Neal McBurnett</i>	
Rounding Considered Harmful	189
<i>Carsten Schürmann</i>	
Author Index	203