Lecture Notes in Computer Science 9269

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

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

Rolf Haenni · Reto E. Koenig
Douglas Wikström (Eds.)

E-Voting and Identity

5th International Conference, VoteID 2015
Bern, Switzerland, September 2–4, 2015
Proceedings

Springer

Editors
Rolf Haenni
Bern University of Applied Sciences
Biel
Switzerland

Reto E. Koenig
Bern University of Applied Sciences
Biel
Switzerland

Douglas Wikström
Royal Institute of Technology
Stockholm
Sweden

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-22269-1 ISBN 978-3-319-22270-7 (eBook)
DOI 10.1007/978-3-319-22270-7

Library of Congress Control Number: 2015944731

LNCS Sublibrary: SL4 – Security and Cryptology

Springer Cham Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at VoteID 2015, the fifth edition of the International Conference on E-Voting and Identity held during September 2–4, 2015, in Bern, Switzerland. Previous VoteID conferences were held in Guildford, UK (2013), Tallinn, Estonia (2011), Luxembourg (2009), and Bochum, Germany (2007). This year's VoteID conference was hosted by the Bern University of Applied Sciences. There were 17 submissions by authors from 11 different countries. Each submission was reviewed by at least three, and on average 4.3, Program Committee members in a double-blind procedure. The committee decided to accept ten papers. The conference program also included one keynote and three invited talks. The paper submission, reviewing, and proceedings preparation process was supported by the EasyChair conference management tool.

Bringing one of the world's leading e-voting conferences to Switzerland was a long-desired objective of the conference organizers. In Switzerland's long tradtion of federalism and direct democracy, frequent referendums are held on national, cantonal, and communal levels. Citizens can vote about changes to the constitution or about accepting new laws up to four times a year. This guarantees not only a maximum amount of self-determination to the citizens, but is also an important stabilizing factor for the political system of the country. In addition to the frequent referendums, regular elections take place on all federal levels, usually every four years. Traditionally, voting used to take place either at the ballot box in local election offices or at the cantonal assembly (called *Landsge- meinde*) in a public space by raising hands. Both traditional voting channels still exist today, but their importance has descreased with the general introduction of postal voting on a national level in 1994. Today, postal voting is the most common form of voting in Switzerland and is widely accepted.

Given the high frequency of referendums and elections, providing the most efficient voting channels to Swiss voters is an obvious objective of Swiss election administrations on all levels. It is therefore not surprising that Switzerland has been a pioneering country not only in postal voting, but also in introducing remote voting over the Internet. The first pilots in the cantons of Geneva and Zurich started almost 15 years ago, and another pilot in the canton of Neuchâtel followed a few years later. All three systems are still in use today and are used by multiple cantons. Just recently, they all received a major update in the underlying security concept by introducing individual verifiability based on confirmation codes. Further updates toward universal verifiability are planned for the near future. The results of scientific research have therefore found fertile soil in Switzerland's fundamental democratic processes.

To establish a link between this year's conference location and the general conference topic, we invited Barbara Perriard, Head of the Political Rights Section of the Federal Chancellery, to give a keynote talk on "Vote électronique: The Long Path Towards the Digitalization of Political Rights." She presented the past and the future of the Swiss e-voting projects and outlined the strategy of the federal administration

and the cantons. We also invited Dr. Uwe Serdült from the Centre for Democracy Studies Aarau (ZDA) to give a talk on "The Use and Users of Swiss Internet Voting." He presented Switzerland's experience with e-voting from a political science perspective. On the more technical side of the topic, we had two invited talks by Prof. Alex Halderman from the University of Michigan on "Security Analysis of Estonia's Internet Voting System" and by Prof. Steve Schneider from the University of Surrey on "Verifiable Voting in Victoria: The vVote Project."

We would like to thank everyone who helped in bringing this conference together: the VoteID Steering Committee for their trust in putting this year's edition into our hands; the authors for their submissions; the Program Committee and the external reviewers for their conscientious and timely efforts in reviewing and discussing the submissions; the keynote speaker for her insights into the process of introducing electronic voting in Switzerland; the invited speakers for delivering high-quality presentations on current research issues; the administration of the Swiss Federal Palace for offering a free guided tour to all participants; and Scytl for their generous sponsorship that allowed us to extend the list of invited speakers and to support students in attending the conference. Finally, we thank our home institution, the Bern University of Applied Sciences, for its support.

June 2015

Rolf Haenni
Reto E. Koenig
Douglas Wikström

Organization

Program Committee

Michael Alvarez	California Institute of Technology, USA
Roberto Araujo	Universidade Federal do Pará, Brazil
David Bernhard	University of Bristol, UK
David Bismark	Votato
Jeremy Clark	Concordia University, Canada
Chris Culnane	University of Surrey, UK
Eric Dubuis	Bern University of Applied Sciences, Switzerland
Aleks Essex	University of Waterloo, Canada
J. Paul Gibson	Telecom & Management SudParis, France
Kristian Gjøsteen	Norwegian University of Science and Technology, Norway
Rajeev Gore	The Australian National University, Australia
Jens Groth	University College London, UK
Rolf Haenni	Bern University of Applied Sciences, Switzerland
Hugo Jonker	University of Luxembourg, Luxembourg
Reto E. Koenig	Bern University of Applied Sciences, Switzerland
Robert Krimmer	Tallinn University of Technology, Estonia
Ralf Kuesters	University of Trier, Germany
Tal Moran	IDC Herzliya
Stephan Neumann	TU Darmstadt, Germany
Olivier Pereira	Université Catholique de Louvain, Belgium
Peter 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
Philip Stark	University of California, Berkeley, USA
Vanessa Teague	The University of Melbourne, Australia
Melanie Volkamer	TU Darmstadt, Germany
Poorvi Vora	The George Washington University, USA
Roland Wen	The University of New South Wales, Australia
Douglas Wikström	KTH Royal Institute of Technology, Sweden
Filip Zagorski	Wroclaw University of Technology, Poland
Dimitrios Zissis	University of the Aegean, Greece

Local Organizers

Eric Dubuis	Bern University of Applied Sciences, Switzerland
Stephan Fischli	Bern University of Applied Sciences, Switzerland
Rolf Haenni	Bern University of Applied Sciences, Switzerland
Severin Hauser	Bern University of Applied Sciences, Switzerland
Reto E. Koenig	Bern University of Applied Sciences, Switzerland
Philipp Locher	Bern University of Applied Sciences, Switzerland

Additional Reviewers

Chaidos, Pyrros
Müller, Johannes
Ronquillo, Lorena
Vogt, Andreas

Contents

Real-World Election Systems

2015 Neuchâtel's Cast-as-Intended Verification Mechanism 3
David Galindo, Sandra Guasch, and Jordi Puiggalí

Log Analysis of Estonian Internet Voting 2013–2014 19
Sven Heiberg, Arnis Parsovs, and Jan Willemson

The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election 35
J. Alex Halderman and Vanessa Teague

Advanced Voting Protocols

Extending Helios Towards Private Eligibility Verifiability 57
Oksana Kulyk, Vanessa Teague, and Melanie Volkamer

Verifiable Internet Elections with Everlasting Privacy and Minimal Trust. . . . 74
Philipp Locher and Rolf Haenni

Vote Validatability in Mix-Net-Based eVoting 92
Pedro Bibiloni, Alex Escala, and Paz Morillo

Making Code Voting Secure Against Insider Threats Using Unconditionally Secure MIX Schemes and Human PSMT Protocols 110
Yvo Desmedt and Stelios Erotokritou

Other Topics

Document Analysis Techniques for Automatic Electoral Document Processing: A Survey 129
J. Ignacio Toledo, Jordi Cucurull, Jordi Puiggalí, Alicia Fornés, and Josep Lladós

Machine-Checked Reasoning About Complex Voting Schemes Using Higher-Order Logic 142
Jeremy E. Dawson, Rajeev Goré, and Thomas Meumann

Experience Reports

Challenging an E-voting System in Court: An Experience Report 161
Richard Hill

Author Index 173