Lecture Notes in Computer Science 7187

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

Aggelos Kiayias Helger Lipmaa (Eds.)

E-Voting and Identity

Third International Conference, VoteID 2011
Tallinn, Estonia, September 28-30, 2011
Revised Selected Papers

Springer

Volume Editors

Aggelos Kiayias
National and Kapodistrian University of Athens
Department of Informatics and Telecommunications
Panepistimiopolis, 15784 Athens, Greece
E-mail: aggelos@di.uoa.gr

Helger Lipmaa
University of Tartu, Institute of Computer Science
J. Liivi 2, 50409 Tartu, Estonia
E-mail: helger.lipmaa@gmail.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-32746-9 e-ISBN 978-3-642-32747-6
DOI 10.1007/978-3-642-32747-6
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012944270

CR Subject Classification (1998): E.3, D.4.6, K.6.5, C.2, J.1, K.4.4, K.5.2

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

These are the proceedings of VoteID 2011, the third in the series of International Conferences on E-Voting and Identity. The conference was held in Tallinn, Estonia, during September 28–30, 2011. The previous two VoteID conferences were held in 2007 (Bochum) and 2009 (Luxembourg). Since then, several countries have moved forward (and a few, backward) on e-voting. In particular, Estonian parliamentary e-voting in Spring of 2011 resulted both in a record number of remote votes (140,846 voters chose to vote remotely) and new controversies. In parallel, Norway has gone forward to start its own remote e-voting process. The current proceedings contain papers that describe both systems.

Since e-voting is already applied in the real world (and often, we have to say, not in an ideally secure way), research on e-voting is gaining in importance. We hope that VoteID 2011 helped not only to further academic research on e-voting, but also to tighten the contacts between the theory and the practice of the discipline. In particular, the Program Committee accepted works on both theoretical and practical aspects ("experience" or system-oriented papers). Moreover, the two invited talks, one by Henrik Nore and Ida Stenerud and the second one by Jens Groth, were explicitly chosen to reflect both sides of e-voting research. We would like to thank the invited speakers for accepting our invitation and for delivering excellent talks. In addition, VoteID 2011 has a panel on "Verifiable E-Voting and Real World," and we would like to thank the panelists (Tarvi Martens, Kristian Gjøsteen, Henrik Nore, Alexander Trechsel, and Andrew Regenscheid) for participation. The Program Committee selected 15 papers for presentation at the conference out of a total of 33 anonymous submissions. Each submission was reviewed by at least three Program Committee members, while Program Committee submissions were reviewed by at least four Program Committee members.

We would like to thank everyone who helped make this conference happen. Our thanks go to the Program Committee and their subreviewers, as listed on the following pages. The submission and review process was greatly simplified by the Web submission and review software written by Shai Halevi. We thank all the submitters as well as the authors for revising their papers accordingly to the reviewers' suggestions. The revised versions were not checked by the Program Committee so the authors bear full responsibility for their contents. We thank Nikolaos Karvelas of the University of Athens and the staff at Springer for their help with producing the proceedings.

VoteID 2011 was generously supported by Scytl. We note that these proceedings include a paper authored by Scytl employees. This contribution was evaluated by the Program Committee entirely independently of the company's support. In the local organization, the General Chair (H. Lipmaa) was helped very professionally by a team, lead by Kerli Kangro, from the conference center of the Tallinn University.

January 2012

Aggelos Kiayias
Helger Lipmaa

VoteID 2011

The Third International Conference on E-voting and Identity 2011

Tallinn, Estonia
September 28–30, 2011

Program Chairs

Aggelos Kiayias	University of Athens, Greece
Helger Lipmaa	University of Tartu, Estonia

Program Committee

Josh Benaloh	Microsoft Research, USA
Felix Brändt	Technische Universität München, Germany
Yvo Desmedt	University College London, UK
Edith Elkind	Nanyang Technological University, Singapore
Jens Groth	University College London, UK
Joseph Lorenzo Hall	UC Berkeley and Princeton, USA
Hugo Jonker	University of Luxembourg, Luxembourg
Aggelos Kiayias	University of Connecticut, USA
Helger Lipmaa	University of Tartu, Estonia
Tal Moran	Harvard, USA
Rene Peralta	NIST, USA
Olivier Pereira	Université Catholique de Louvain, Belgium
Mark Ryan	University of Birmingham, UK
Peter Ryan	University of Luxembourg, Luxembourg
Berry Schoenmakers	University of Eindhoven, The Netherlands
Jörg Schwenk	Ruhr-Universität Bochum, Germany
Vanessa Teague	University of Melbourne, Australia
Melanie Volkamer	TU Darmstadt, Germany
Moti Yung	Columbia University and Google, USA

External Reviewers

Haris Aziz
Catherine Baker
Stephanie Bayer
Markus Brill
Marco Cova
Chris Culnane
Denise Demirel
Naipeng Dong
Richard Frankland
Kristian Gjøsteen
Paul Harrenstein
Simon Kramer
Dalia Khader
Gabriele Lenzini
Maina Olembo
Doron Peled
Ariel Procaccia
Kim Ramchen
Michael Schläpfer
Hans Georg Seedig
Nicolas Troquard
Dominique Unruh

Table of Contents

Experiences