Lecture Notes in Computer Science 4896

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

Ammar Alkassar Melanie Volkamer (Eds.)

E-Voting and Identity

First International Conference, VOTE-ID 2007
Bochum, Germany, October 4-5, 2007
Revised Selected Papers

Volume Editors

Ammar Alkassar
Sirrix AG security technologies
Im Stadtwald D3.2, 66123 Saarbrücken, Germany
E-mail: a.alkassar@sirrix.com

Melanie Volkamer
University of Passau, Institute of IT-Security and Security Law
Innstr. 43, 94032 Passau, Germany
E-mail: volkamer@uni-passau.de

Library of Congress Control Number: 2007941815

CR Subject Classification (1998): E.3, D.4.6, C.2, J.1, H.2.0, K.5.2, K.6.5, K.4.4

LNCS Sublibrary: SL 4 – Security and Cryptology

ISSN 0302-9743
ISBN-10 3-540-77492-0 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-77492-1 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12210206 06/3180 5 4 3 2 1 0

Foreword

Voting and identity have a very delicate relationship. Only a few processes depend so much on an identity management respecting the fine line between reliable identification and reliable non-identifiability each at its part during the process. And only a few processes may change their outer appearance so much with the advent of new IT as voting and identity management do.

So it was no surprise in FIDIS, the interdisciplinary Network of Excellence working on the Future of Identity in the Information Society, when Ammar Alkassar proposed analyze the technical, socio-ethical and legal relations between Identity and E-Voting as part of Sirrix's activity in FIDIS.

There are many reasons for doing this, e.g., the open question of the implications of identity and identification to the emerging field of E-Government and E-Democracy, especially E-Voting. Issues to be discussed are from several domains, e.g., is identity fraud a crucial matter in E-Voting? What is the trade-off between anonymity and free speech vs. content-related offences? Is it appropriate to use ID cards or health-insurance cards with digital identities for citizen tasks or voting? What about using SIM cards? Can we employ biometrics for identification purposes with respect to E-Democracy?

Last but not least nearly all areas of E-Government rely on a reliable link between the citizens and their governments and administrations. However, in contrast to business processes, the effects are much more crucial: Identity fraud may cause more problems than in the business domain; the consequences of misuse cannot be measured just by financial means.

With these and many other issues at stake it was great to see VOTE-ID 2007 become such a great success with high-quality papers and discussions. It is a great pleasure to thank all the submitters, the Program Committee, and especially the Program Chairs Ammar Alkassar (Sirrix AG security technologies) and Melanie Volkamer (Institute of IT-Security and Security Law, University Passau) for the tremendous work in getting this conference off the ground.

November 2007

Kai Rannenberg
Goethe University Frankfurt
FIDIS Co-ordination

Preface

Electronic voting has been one of the most controversial topics of discussion in the IT security community for the past 20 years. During the 1980s, the discussion was characterized by the development of new, powerful cryptographic schemes and protocols. These were driven by the necessity to meet the requirements for replacing the former analog systems with newer election systems and e-voting technologies.

However, recurring problems with the election systems that were deployed, as well as inherent weaknesses, have burdened the argument for pushing forward. Now, after what could be characterized as a turbulent wave of pros and cons, the discussion focus has moved to address how the democratic spirit of elections can be respected in full, while also gaining the confidence of the public in the latest voting systems.

With respect to this new discussion, it was quite natural for the FIDIS Network of Excellence (NoE) to address the topic of E-Voting and Identity as well as its relevance in democratic society.

"Future of IDentity in the Information Society" (FIDIS) is a project funded by the European Commission. The network consists of 24 partners from 11 European countries collaborating on topics such as privacy, data protection, profiling and identity in both the public and private sectors.

An important aspect of the FIDIS NoE, as well as the recent conference, is to provide a highly-interdisciplinary forum for researchers stemming from various fields and organizations. Hence, the Program Committee was selected to represent leading experts in the related areas of cryptography, voting systems and ID management as well as legal and social sciences.

The conference was successful in bringing together researchers from universities and research institutes as well as practitioners from industry and electoral boards to discuss the central aspects of e-voting as well as the more pragmatic issues.

We would like to thank Berry Schoenmakers from the Technical University in Eindhoven (The Netherlands) for his excellent keynote on "E-Voting Crises" and also the panel members of the panel discussion: Klaus Brunnstein (University of Hamburg, Germany), Hans van Wijk (NEDAP, The Netherlands), Robert Stein (Head of Election Division, Federal Ministry of Interior, Austria) and Craig Burton (Everyone Counts).

We would like to extend a special thanks to Cline Fischer, who was kind enough to arrange the conference venue and take care of the administrative tasks which allowed the conference to run so smoothly. The conference was hosted by Sirrix AG and held at the European Center for IT-Security in Bochum.

November 2007

Ammar Alkassar
Melanie Volkamer

Organization

Program Chairs

Ammar Alkassar	Sirrix AG, Germany
Melanie Volkamer	Passau University, Germany

Program Committee

Josh Benaloh	Microsoft, USA
Rüdiger Grimm	Koblenz-Landau University, Germany
Marit Hansen	ICPP, Germany
Dirk Heckmann	Passau University, Germany
David-Olivier Jaquet-Chiffelle	University of Applied Sciences of Bern, Switzerland
Frank Koob	German Federal Office for Information Security, Germany
Robert Krimmer	evoting.cc, Austria
Ronald Leenes	Tilburg University, Netherlands
Helger Lipmaa	University College London, UK
Sjouke Mauw	Luxemburg University, Luxemburg
Margaret McGaley	NUI Maynooth, Ireland
Lilian Mitrou	University of the Aegean, Greece
Olivier Pereira	Université Catholique de Louvain, Belgium
Günther Pernul	Regensburg University, Germany
Andreas Pfitzmann	Dresden Technical University, Germany
Bart Preneel	Catholic University Leuven, Belgium
Kai Rannenberg	Frankfurt University, Germany
Peter Ryan	Newcastle University, UK
Ahmad-Reza Sadeghi	Ruhr University Bochum, Germany
Joseph Savirimuthu	Liverpool University, UK
Berry Schoenmakers	Eindhoven Technical University, Netherlands

Additional Reviewers

Roberto Araujo, Stefan Berthold, Sebastian Clauß, André Deuker, Stefan Duerbeck, Ludwig Fuchs, Sebastian Gajek, Yacine Gasmi, Jörg Gilberg, Jörg Helbach, Hugo Jonker, Andreas Juschka, Jan Kolter, Michael Kreutzer, Katja Liesebach, Olivier de Marneffe, Denis Royer, Hans Loehr, Tobias Scherner, Patrick Stewin, Martin Unger, Stefan Weber, Jan Zibuschka, Felix Zimmermann

Table of Contents

Improvements/Extensions of Existing Approaches

Code Voting