

REAL-WORLD

ELECTRONIC VOTING

DESIGN, ANALYSIS AND DEPLOYMENT

CRC Series in Security, Privacy and Trust

SERIES EDITORS

Jianning Zhou

Institute for Infocomm Research, Singapore

jyzhou@i2r.a-star.edu.sg

Pierangela Samarati

Universita' degli Studi di Milano, Italy

pierangela.samarati@unimi.it

AIMS AND SCOPE

This book series presents the advancements in research and technology development in the area of security, privacy, and trust in a systematic and comprehensive manner. The series will provide a reference for defining, reasoning and addressing the security and privacy risks and vulnerabilities in all the IT systems and applications, it will mainly include (but not limited to) aspects below:

- Applied Cryptography, Key Management/Recovery, Data and Application Security and Privacy;
- Biometrics, Authentication, Authorization, and Identity Management;
- Cloud Security, Distributed Systems Security, Smart Grid Security, CPS and IoT security;
- Data Security, Web Security, Network Security, Mobile and Wireless Security;
- Privacy Enhancing Technology, Privacy and Anonymity, Trusted and Trustworthy Computing;
- Risk Evaluation and Security Certification, Critical Infrastructure Protection;
- Security Protocols and Intelligence, Intrusion Detection and Prevention;
- Multimedia Security, Software Security, System Security, Trust Model and Management;
- Security, Privacy, and Trust in Cloud Environments, Mobile Systems, Social Networks, Peer-to-Peer Systems, Pervasive/Ubiquitous Computing, Data Outsourcing, and Crowdsourcing, etc..

PUBLISHED TITLES

Location Privacy in Wireless Sensor Networks

Ruben Rios, Javier Lopez, and Jorge Cuellar

Real-World Electronic Voting: Design, Analysis and Deployment

Feng Hao and Peter Y. A. Ryan

Touchless Fingerprint Biometrics

Ruggero Donida Labati, Vincenzo Piuri, and Fabio Scotti

CRC Series in Security, Privacy and Trust

REAL-WORLD

ELECTRONIC VOTING

DESIGN, ANALYSIS AND DEPLOYMENT

EDITED BY

FENG HAO AND PETER Y. A. RYAN



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2017 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

Printed on acid-free paper
Version Date: 20161114

International Standard Book Number-13: 978-1-4987-1469-3 (Hardback)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
<http://www.taylorandfrancis.com>

and the CRC Press Web site at
<http://www.crcpress.com>

Contents

Foreword	vii
Preface	xi
SECTION I SETTING THE SCENE	1
1 Software Independence Revisited	3
<i>Ronald L. Rivest and Madars Virza</i>	
2 Guidelines for Trialling E-Voting in National Elections	19
<i>Ben Goldsmith</i>	
SECTION II REAL-WORLD E-VOTING IN NATIONAL ELECTIONS	49
3 Overview of Current State of E-Voting Worldwide	51
<i>Carlos Vegas and Jordi Barrat</i>	
4 Electoral Systems Used around the World	77
<i>Siamak F. Shahandashti</i>	
5 E-Voting in Norway	103
<i>Kristian Gjøsteen</i>	

6	E-Voting in Estonia	129
	<i>Dylan Clarke and Tarvi Martens</i>	
7	Practical Attacks on Real-World E-Voting	143
	<i>J. Alex Halderman</i>	
SECTION III E2E VOTING SYSTEM AND REAL-WORLD APPLICATIONS		171
8	An Overview of End-to-End Verifiable Voting Systems	173
	<i>Syed Taha Ali and Judy Murray</i>	
9	Theoretical Attacks on E2E Voting Systems	219
	<i>Peter Hyun-Jeen Lee and Siamak F. Shahandashti</i>	
10	The Scantegrity Voting System and Its Use in the Takoma Park Elections	237
	<i>Richard T. Carback, David Chaum, Jeremy Clark, Aleksander Essex, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T. Sherman, Poorvi L. Vora, John Wittrock and Filip Zagórski</i>	
11	Internet Voting with Helios	277
	<i>Olivier Pereira</i>	
12	Prêt à Voter — The Evolution of the Species	309
	<i>Peter Y. A. Ryan, Steve Schneider, and Vanessa Teague</i>	
13	DRE-i and Self-Enforcing E-Voting	343
	<i>Feng Hao</i>	
14	STAR-Vote: A Secure, Transparent, Auditable and Reliable Voting System	375
	<i>Susan Bell, Josh Benaloh, Michael D. Byrne, Dana DeBeauvoir, Bryce Eakin, Gail Fisher, Philip Kortum, Neal McBurnett, Julian Montoya, Michelle Parker, Olivier Pereira, Philip B. Stark, Dan S. Wallach and Michael Winn</i>	
	References	405
	Index	453