

Feng Hao and Peter Y A Ryan (Eds.)

***Real-World Electronic
Voting: Design, Analysis
and Deployment***



Contents

Foreword	xvii
Preface	xxi
SECTION I: SETTING THE SCENE	1
1 Software Independence Revisited	3
<i>Ronald L. Rivest and Madars Virza</i>	
1.1 Introduction	4
1.2 Problem: Software complexity of voting systems	4
1.2.1 The difficulty of evaluating complex software for errors	5
1.2.2 The need for software-independent approaches	6
1.3 Definition and rationale for software-independence	6
1.3.1 Refinements and elaborations of software-independence	7
1.3.2 Examples of software-independent approaches	8
1.4 How does one test for software-independence?	9
1.5 Discussion	10
1.5.1 Implications for testing and certification	10
1.5.2 Related issues	10
1.6 Evidence-based elections	11
1.7 The use of a public ledger	11
1.8 End-to-end verifiable voting systems	13
	iii

1.9	Program verification	15
1.10	Verifiable computation and zero-knowledge proofs	16
1.11	Conclusions and suggestions	17
2	Guidelines for Trialling E-voting in National Elections	19
	<i>Ben Goldsmith</i>	
2.1	Terminology	20
2.2	Context for E-Voting	21
2.3	International Electoral Standards	23
2.4	Decision in Principle	28
2.4.1	Decision in Principle Foundations	28
2.4.1.1	Feasibility Study Mandate	28
2.4.1.2	Vendor Relations	29
2.4.2	Feasibility Study Committee Working Groups	30
2.4.2.1	Issue 1 – Assessment of the Current System of Voting and Counting	30
2.4.2.2	Issue 2 – Assessment of the Advantages and Disadvantages Offered by Voting Technologies	31
2.4.2.3	Issue 3 – Review of IT Security Aspects	31
2.4.2.4	Issue 4 – Determining Technical Feasibility	32
2.4.2.5	Issue 5 – Cost Benefit Analysis	33
2.4.2.6	Issue 6 – Institutional Capacity	34
2.4.2.7	Issue 7 – Legal Reform Issues	35
2.4.3	Study Trips	35
2.4.4	Vendor Demonstration	36
2.4.5	Stakeholder Consultation	36
2.4.6	Decision in Principle	37
2.5	Pilot Project Prerequisites	38
2.5.1	Pilot Project Mandate	38
2.5.1.1	Type of Pilot	38
2.5.1.2	Pilot Locations	39
2.5.1.3	Solutions Being Piloted	39
2.5.2	Legislation	40
2.5.3	Electronic Voting Technology Specification	40

2.5.4	Pilot Project Funding	41
2.6	Pilot Project	42
2.6.1	Managing the Pilot Project	42
2.6.2	Procuring Electronic Voting Technologies	42
2.6.3	Testing and Certification	43
2.6.4	Polling and Counting Procedures	43
2.6.5	Voter Education	44
2.6.6	Training	44
2.6.7	Stakeholder Outreach	44
2.6.8	Election Day Support	45
2.6.9	Observation of the Pilot Project	45
2.6.10	Mandatory Audit	46
2.6.11	Pilot Project Evaluation	46
2.7	The Decision on Adoption	47

SECTION II: REAL-WORLD E-VOTING IN NATIONAL ELECTIONS 51

3 Overview of Current State of E-voting World-wide 53

Carlos Vegas and Jordi Barrat

3.1	Introduction	54
3.2	The Public Nature of Elections	55
3.3	Civic Activism	61
3.4	Business as Usual	64
3.5	Outdated Technologies	68
3.6	The Political Context	70
3.7	Voters Matter	74
3.8	Conclusions	77

4 Electoral Systems Used around the World 79

Siamak F. Shahandashti

4.1	Introduction	80
4.2	Some Solutions to Electing A Single Winner	81
4.3	Some Solutions to Electing Multiple Winners	84

4.4	Blending Systems Together	89
4.5	Other Solutions	90
4.6	Which Systems Are Good?	92
4.6.1	A Theorist’s Point of View	92
4.6.1.1	Majority Rules	92
4.6.1.2	Bad News Begins	93
4.6.1.3	Arrow’s Impossibility Theorem	95
4.6.1.4	Gibbard–Satterthwaite Impossibility Theorem	96
4.6.1.5	Systems with Respect to Criteria	98
4.6.2	A Practitioner’s Point of View	100
5	E-voting in Norway	105
	<i>Kristian Gjøsteen</i>	
5.1	Introduction	105
5.2	Elections in Norway	106
5.3	Requirements	109
5.4	Buying a Voting System	110
5.5	Cryptographic Protocol	114
5.5.1	Scytl’s Proposal	114
5.5.2	Modifications	118
5.5.3	The Modified Protocol	120
5.6	Deployment	124
5.6.1	The 2011 Election	124
5.6.2	The 2013 Election	126
5.7	Concluding Remarks	129
6	E-voting in Estonia	131
	<i>Dylan Clarke and Tarvi Martens</i>	
6.1	Voting in Estonia	132
6.2	Estonian National ID Cards	134
6.3	The Internet Voting System	136
6.3.1	System Components	137
6.3.2	Normal System Operation	137

6.3.3	Auditing and Verification Capabilities	139
6.4	Internet Voting Assumptions and Reception	141
6.5	System Performance	143
7	Practical Attacks on Real-world E-voting	145
	<i>J. Alex Halderman</i>	
7.1	Introduction	145
7.2	Touchscreen DREs	147
7.2.1	Diebold	147
7.2.2	Top to Bottom	151
7.2.3	The Test of Time	152
7.2.4	Around the World	154
7.3	Internet Voting	159
7.3.1	The Washington, D.C. Internet Voting System	160
7.3.2	Estonia's Internet Voting System	165
7.3.3	The New South Wales iVote System	167
7.4	Conclusion	171

SECTION III E2E VOTING SYSTEM AND REAL-WORLD APPLICATIONS 173

8 An Overview of End-to-End Verifiable Voting Systems 175

Syed Taha Ali and Judy Murray

8.1	Introduction	176
8.2	Security Properties of Voting Systems	178
8.2.1	Vote Privacy	178
8.2.2	Vote Verifiability	179
8.2.3	Other Properties	180
8.2.4	Conflicts and Challenges	181
8.3	Cryptographic E2E Voting Systems	181
8.3.1	Precinct-based Voting with Physical Ballots	182
8.3.1.1	Voteegrity	182
8.3.1.2	Prêt à Voter	186
8.3.1.3	Punchscan	187

8.3.1.4	Scantegrity	188
8.3.1.5	Scratch & Vote	190
8.3.2	Precinct-based Voting with Electronic Ballots	192
8.3.2.1	MarkPledge	192
8.3.2.2	Bingo Voting	194
8.3.2.3	Voter Initiated Auditing	195
8.3.2.4	VoteBox	196
8.3.2.5	Wombat	197
8.3.2.6	STAR-Vote	199
8.3.2.7	DRE-i	200
8.3.3	Remote Voting with Electronic Ballots	200
8.3.3.1	Adder	201
8.3.3.2	JCJ and Civitas	201
8.3.3.3	Helios	203
8.3.3.4	Pretty Good Democracy	205
8.3.3.5	Remotegrity	206
8.4	Non-cryptographic E2E Voting Systems	208
8.4.0.1	ThreeBallot, VAV, and Twin	208
8.4.0.2	Randell & Ryan’s Scratch Card Voting System	209
8.4.0.3	Aperio	210
8.5	The Way Forward for E2E Voting Systems	212
8.5.1	Technical Issues	213
8.5.2	Usability	214
8.5.3	Legal Framework	215
8.5.4	Uptake of E2E Voting Systems	217
8.6	Conclusion	218
8.7	Acknowledgements	218
9	Theoretical Attacks on E2E Voting Systems	219
	<i>Peter Hyun-Jeen Lee and Siamak F. Shahandashti</i>	
9.1	Introduction	220
9.2	Integrity	221
9.2.1	Misprinted ballots attack	221

9.2.2	Trash Attack	222
9.2.3	Clash Attack	223
9.2.4	Flawed Mix-net	224
9.3	Privacy	226
9.3.1	Replay Attack	226
9.3.2	Kleptographic Attack	228
9.3.3	Pfitzmann’s attack	229
9.3.4	Duplicate ciphertext attack	230
9.3.5	Breaking privacy without detection	230
9.4	Coercion	231
9.4.1	Forged ballot	232
9.4.2	Vote against a candidate	232
9.4.3	Scratch-off card attack	232
9.4.4	Spoiling ballots	233
9.4.5	Pay-Per-Mark & Pay-for-Receipt	235
9.5	Conclusion	236
9.6	Acknowledgements	236

10 The Scantegrity Voting System and its Use in the Takoma Park Elections 237

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

10.1	Introduction	239
10.1.1	Key Properties	239
10.1.2	Outline	241
10.1.3	Organization of this chapter	241
10.2	The Punchscan Voting System	242
10.2.1	Voter Experience	242
10.2.2	Election Set-Up	242
10.2.3	Ballot Printing and Voter Privacy	244
10.2.4	The First Binding E2E Election	245
10.2.5	Lessons Learned	246
10.3	The Scantegrity II Voting System	247
10.3.1	Ballot Features	247

10.3.2	The Scantegrity Back-End	248
10.3.3	Election Day	250
10.3.4	Posting and Tallying	250
10.3.5	Auditing the Results	252
10.3.6	Dispute Resolution	253
10.4	The 2009 Takoma Park Election	254
10.4.1	Requirements	255
10.4.2	Mock Election	256
10.4.3	The Election	257
10.5	The Remotegrity Voting System	260
10.5.1	Voter Experience	260
10.5.2	Security Properties	262
10.6	Audiotegrity	263
10.6.1	The Voting Process with Audiotegrity	263
10.6.2	Dispute Resolution Properties	264
10.7	Takoma Park Election, 2011	265
10.8	Usability Studies	267
10.8.1	Related Studies	267
10.8.2	Methodology	268
10.8.3	Known Limitations	269
10.8.4	Voter Response	270
10.8.5	Observational Results	272
10.8.6	Election Judge Response	273
10.8.7	Study Findings	273
10.9	Current Status of the Project	275
10.10	Conclusions	275
11	Internet voting with Helios	279
	<i>Olivier Pereira</i>	
11.1	Introduction	280
11.1.1	Helios History	282
11.2	Election walkthrough	282
11.2.1	Voting in a Helios election	283

11.2.1.1	Invitation to vote	283
11.2.1.2	Submitting a ballot	283
11.2.2	Election management	285
11.2.2.1	Election creation	285
11.2.2.2	Election tally	287
11.2.3	Election audit	288
11.2.3.1	Cast-as-intended verification	288
11.2.3.2	Recorded-as-cast verification	291
11.2.3.3	Tallied-as-recorded verification	292
11.3	The use of cryptography in Helios	293
11.3.1	Arithmetic and computational assumption	293
11.3.2	Encryption	293
11.3.3	Zero-Knowledge proofs	295
11.3.3.1	Sigma protocols	295
11.3.3.2	Proving honest key generation	296
11.3.3.3	Proving correct decryption	297
11.3.3.4	Proving ballot validity	298
11.3.4	Protocol analysis	299
11.3.4.1	Works on Verifiability	300
11.3.4.2	Works on ballot privacy	301
11.3.4.3	Miscellaneous works	301
11.4	Web application perspective	302
11.4.1	The browser interface	302
11.4.2	Cryptography in the browser	303
11.4.3	Application security	304
11.5	Helios variants and related systems	305
11.5.1	Mixnet-based variants	305
11.5.2	Variants aiming at countering ballot-stuffing	306
11.5.3	Variants aiming at perfectly private audit data	306
11.5.4	Variants based on full threshold encryption	307
11.5.5	Variant supporting vote delegation	307
11.5.6	Alternate Helios frontends	308
11.5.7	Audit tools	308

11.6 Conclusion	309
---------------------------	-----

12 Prêt à Voter - the Evolution of the Species 311

Peter Y A Ryan, Steve Schneider, and Vanessa Teague

12.1 Introduction	313
12.1.1 End-to-End Verifiability	314
12.2 Outline of Prêt à Voter	315
12.2.1 The Voting Ceremony	315
12.2.2 Vote Counting	317
12.2.3 Advantages of Prêt à Voter	318
12.3 Auditing the Election	319
12.3.1 Auditing the Ballot Generation Authority	319
12.3.2 Auditing Mixing and Decryption	320
12.3.2.1 Auditing the Mixes	320
12.3.2.2 Auditing the Decryption Tellers	321
12.4 Cryptographic Components	321
12.4.1 Decryption mixes	321
12.4.2 Re-encryption mixnets	322
12.4.2.1 Re-encryption mixes with cyclic shifts	322
12.4.2.2 Re-encryption Mixes with Affine Transformations	323
12.4.2.3 Re-encryption Mixes With Full Permutations	323
12.4.3 Distributed generation of ballots	324
12.4.4 The bulletin board	324
12.5 Facilitating verification and privacy	325
12.5.1 Encouraging cast-as-intended verification (Ballot auditing)	325
12.6 Enhancing robustness using parallel verification mechanisms	326
12.6.1 Verified Encrypted Paper Audit Trails	327
12.6.2 Human Readable Paper Audit Trails	327
12.6.3 Confirmation codes and signatures	328
12.7 Accountability, dispute resolution and Resilience	329
12.7.1 Cast-as-Intended Verification	329
12.7.2 Authenticity of Receipts (included-as-cast verification)	330
12.7.3 Tally verification	331

12.8	Vulnerabilities and Counter-measures	331
12.8.1	Ballot Stuffing	331
12.8.2	Information Leakage	332
12.8.3	Retention of the Candidate List	332
12.8.4	Forced/Coerced Randomisation	333
12.8.5	Chain Voting	333
12.8.6	Trash Attacks	334
12.8.7	Clash Attacks	334
12.8.8	Psychological Attacks	334
12.9	Prêt à Voter Goes Down-Under	335
12.9.1	Significance of the VEC Election	335
12.9.2	Challenges of combining end-to-end verifiability with tradi- tional Victorian paper voting	336
12.9.3	Specific Design choices	337
12.9.3.1	Computer-assisted voting	337
12.9.3.2	Unified Scanner and EBM	337
12.9.4	Handling complex ballots and printing them on demand. . .	338
12.9.5	The Web Bulletin Board	338
12.9.6	vVote-specific vulnerabilities and countermeasures	340
12.9.7	Practical experiences	341
12.10	Conclusions	342
13	DRE-i and Self-Enforcing E-Voting	345
	<i>Feng Hao</i>	
13.1	Introduction	346
13.2	Dining Cryptographers problem	347
13.2.1	Description of the problem	347
13.2.2	Chaum's original solution: DC-net	348
13.2.3	Limitations of DC-net	348
13.2.4	First attempt on a new solution	350
13.2.5	Improved solution: AV-net	351
13.2.6	Presentation at SPW 2006	353
13.3	Boardroom electronic voting	354

- 13.3.1 Open Vote protocol 355
- 13.3.2 Extension to multi-candidate election 356
- 13.3.3 Presentation at WISSec 2009 357
- 13.4 Large-scale electronic voting 358
 - 13.4.1 From decentralized to centralized 358
 - 13.4.2 Trade-off 359
 - 13.4.3 Direct Recording Electronic with Integrity 359
 - 13.4.3.1 Setup 360
 - 13.4.3.2 Voting 361
 - 13.4.3.3 Tallying 363
 - 13.4.4 Publication of the DRE-i paper 364
- 13.5 Trial elections 364
 - 13.5.1 Prototyping DRE-i 364
 - 13.5.2 Favourite chocolate election 365
 - 13.5.3 Favourite cheese election 366
 - 13.5.4 ERC Starting Grant on Self-Enforcing E-Voting 370
 - 13.5.5 A Verifiable Classroom Voting system 371
 - 13.5.6 Cryptography Meeting Pedagogy 374
- 13.6 Conclusion 375

14 STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System 377

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

- 14.1 Introduction 379
- 14.2 Voter Flow 381
- 14.3 Design 384
 - 14.3.1 Crypto Overview 385
 - 14.3.2 Triple Assurance 386
 - 14.3.3 Software and Hardware Engineering 387
- 14.4 Usability 388
 - 14.4.1 Design Considerations 388
 - 14.4.2 User Interface Design Specification 391

14.4.3	Issues that still need to be addressed	392
14.5	Audit	393
14.6	The Cryptographic Workflow	395
14.7	Threats	400
14.7.1	Coercion	401
14.7.1.1	Chain voting	401
14.7.1.2	Absentee and provisional ballots	402
14.7.2	Further analysis	403
14.8	Conclusions and Future Work	404
	References	407
	Index	455