More trust in Electronic Voting with E2E Verifiable Voting Systems

CASED

TECHNISCHE UNIVERSITÄT DARMSTADT

Dr. Melanie Volkamer

Increasing trust …

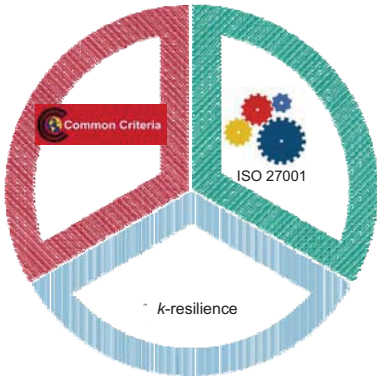
TECHNISCHE UNIVERSITÄT DARMSTADT

... in election results based on electronic voting by ….

… evaluation and certification

TECHNISCHE UNIVERSITÄT DARMSTADT

… based on international standards



https://www.bsi.bund.de/cae/servlet/contentblob/480286/publicationFile/29305/pp0037b_engl_pdf.pdf

… publishing the source code

TECHNISCHE UNIVERSITÄT DARMSTADT

… ideally without any time or location constraints (for instance downloadable from the Internet)

Is this enough?

TECHNISCHE UNIVERSITÄT DARMSTADT

… unfortunately not!

Why?

... because published and evaluated source code is not the same that is used

… because evaluators did not detect a backdoor/ malfunction

… because manipulations cannot be detected

Why verifiable electronic voting systems?

TECHNISCHE UNIVERSITÄT DARMSTADT

One solution VVPATs

TECHNISCHE UNIVERSITÄT DARMSTADT

voter verifiable paper audit trails

… independent verification system to detect possible fraud or malfunction

… is readable by the human eye and voters can directly interpret their vote

… enables manual paper vote count if a recount is necessary

… but a couple of open questions

TECHNISCHE UNIVERSITÄT DARMSTADT

- Manual tallying in how many polling stations in which situations?
- Which result is the legal one?
- What if printer crashes?
- What are the remaining advantages for electronic voting?
- First user studies show: most voters would not discover (malicious) modifications on paper
- Not applicable for remote electronic voting

Alternative solution

TECHNISCHE UNIVERSITÄT DARMSTADT

cryptographic verifiability

- Provides “more” verifiability (namely E2E verifiability)
  - individual verifiability means that the voter can verify that his/her vote is ‘cast as intended’ and ‘stored as cast’
  - universal verifiability means that the voter / everyone can verify that all votes are ‘tallied as stored’

Alternative solution

TECHNISCHE UNIVERSITÄT DARMSTADT

cryptographic verifiability

- Provides more flexibility and is less time intensive
  - observation during the whole day is not required
  - verifiability can be done at any time from any place over the Internet
  - trust in those proceeding the paper audit trails
  - trust that at least some paper audit trails are manual recounted
  - applicable for remote electronic voting

My recommendations

TECHNISCHE UNIVERSITÄT DARMSTADT

- Be as transparent as possible regarding
  - Source code, system descriptions, …
  - Evaluation techniques and bodies
- Reduce trust by implementing verifiability
  - Cryptographic E2E verifiable voting systems in particular for remote electronic voting
  - Proper VVPATs with recounts in randomly chosen polling stations

TECHNISCHE UNIVERSITÄT DARMSTADT

Thank you for your attention!