Mobile-based auditing of the DEMOS 2 e-voting system

Ben Goldsworthy

Overview

- Introduction
- Definitions
- Background
- System Architecture
- Design
- Implementation
- Process Description
- Testing & Evaluation
- Conclusion

Introduction – Project Aims

- To add functionality to facilitate E2E-verifiability to current DEMOS 2 implementation
- To develop Android mobile app. for verifying
- To ensure voter privacy is protected
- To deter voter coercion or buying
- To document data structures used in order to allow future developers to easily produce their own auditing software

Definitions

- Voting – any process of indicating one’s preference(s) out of a number of proposed choices
- Election – the process of presenting choices, recording votes, tallying totals and determining the victor or victors
- Traditional voting system – a non-electronic means of running an election (e.g., paper ballots, raised hands, pottery shards)
- Paper-based electronic voting systems – an otherwise-traditional (specifically paper ballot-based) voting system in which some aspects (e.g., counting, transporting, etc.) are handled electronically

Definitions

- Direct recording electronic (DRE) voting systems – a voting system in which no traditional ballot is produced
- I-voting – a subset of DRE voting systems in which the votes are transmitted over the Internet
- End-to-end (E2E) verifiability – being able to verify that a vote has been *recorded-as-intended*, *cast-as-recorded* and *counted-as-cast*

Background

- A detour for some political philosophy
  - The Kratic Scale
  - Kratic Trees
- ‘Democracy’
- An example election

Background

- Pros of traditional voting systems
  - Resistant to cyber attacks
  - Robust
  - Fulfils first two criteria of E2E-verifiability
- Cons
  - Voters can’t check ballots counted, must trust others to observe count – no *counted-as-cast* verifiability?
  - Voters must travel to polling stations

Background

- Some proposed benefits o introducing e-voting
  - May increase turnout by up to 79%[1]
  - Allows all voters to verify election results, or to delegate responsibility to others
  - May save up to £12.8 million annually[1]
  - Allows more people to vote

Background

- E-voting in practice
  - Out of 196[3] nations (123[2] of which are considered ‘democratic’), only 19 have introduced e-voting systems at some point in time. Of these, 16 still run such systems
  - The first was the United States in 1966
- I-voting in practice
  - 6 nations have thusfar experimented with I-voting
  - France was the first in 2003, allowing certain expatriates to vote over the Internet
  - 3 of these continue to run such systems

Background

- E-voting in the UK
  - The UK has run a few e-voting pilots, with the first in 2000
  - The Digital Democracy Commission's 2015 report[4]
    - 'By 2020, secure online voting should be an option for all voters'
  - However, the government currently 'do not have any plans to introduce electronic voting for statutory elections either using electronic voting in polling booths or remotely via the internet.'[5]

Background

- DEMOS 2
  - Proposed E2E-verifiable I-voting system
  - Development began in 2017
  - Implementation details to follow
  - Lacks auditing software or much of anything *to* audit

System Architecture

- E-voting
  - Voter; tallier; auditor; and trustee
  - Bulletin Board; Election Authority; Registration Authority; and an I-ballot box

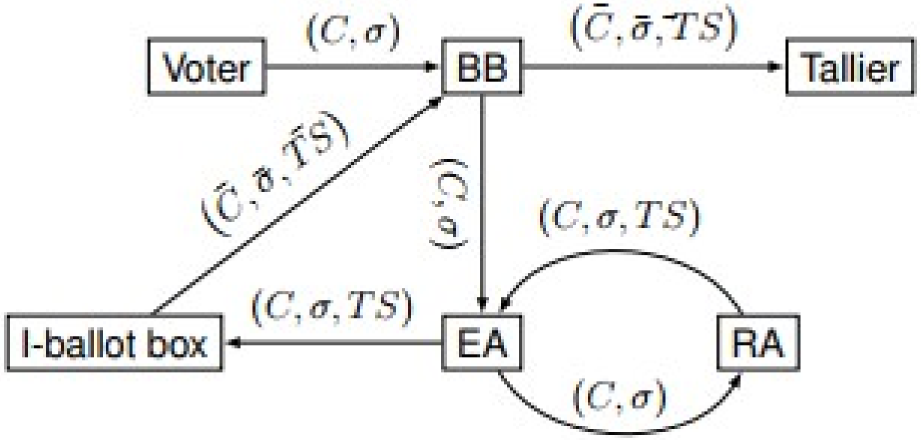

Figure 3.1: Typical e-voting system architecture

System Architecture

- DEMOS 2
  - Node.js Web server
    - Django Web framework
    - Milagro Crypto Javascript
  - Celery distributed task queue
  - MySQL database

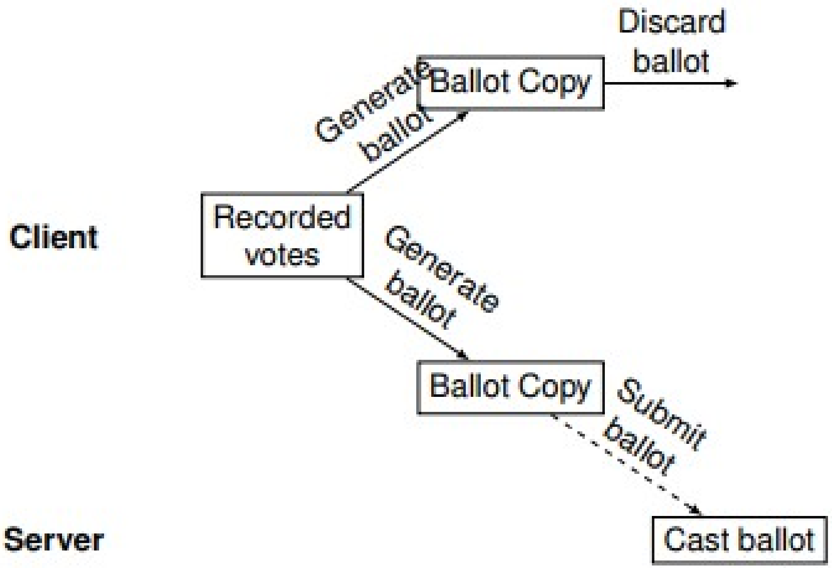

Figure 3.2: From recorded votes to cast ballots

Design

- Requirements – DEMOS 2 & app.
- DEMOS 2 modifications
- Auditor app. Design
- The LBRF

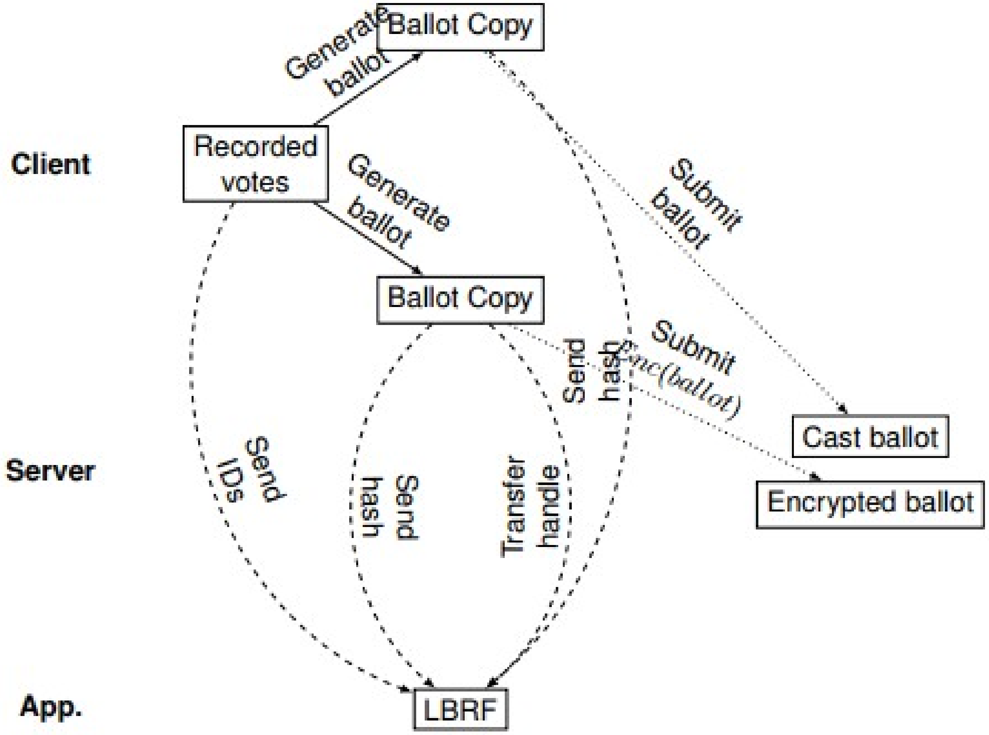

Figure 4.1: From recorded votes to cast ballots, encrypted ballots and LBRFs

Implementation

- See dissertation

Process Description

- See dissertation

Testing & Evaluation

- Limited in what I could test and evaluate
- Tried to describe testing procedure for a theoretical future developer who completes the app.

Conclusion

- Some aims & requirements achieved, most not
- Review of project
  - What *hasn't* been produced
  - What *has*
  - Issues: timekeeping, motivation, understanding, confusion, getting a job

Conclusion

- Ultimately, though, DRE voting systems may not be a good idea
  - Table (see handout) provides reality check on proposed benefits
  - Paper voting lacks only *counted-as-cast* verifiability, voters must trust others to observe count fairness
  - DRE voting adds this, but in such a way that voters *still* have to trust others (or all become crypto experts)
  - In doing so, it also undermines faith in the electoral system, limits the chances of getting fair observers of all political strips and grants corrupt election authorities a prime opportunity to implement flawed systems and interfere with elections
  - Doing all this so that 2-3 astronauts can vote seems like a pretty bad trade-off

End on a high note

- I’ve learnt a lot about e-voting, even if it led to me turning completely against DRE voting
- I’ve gained experience with a number of interesting tools
  - Django
  - Using Git alongside Vincent
  - Android app. development (Javascript & Kotlin)
  - LaTeX

References

1. WebRoots Democracy. *Viral Voting*. 2015
2. *How Many Democratic Nations Are There?* Borgen Magazine. 2013
3. Matt Rosenberg. *The Number of Countries in the World*. ThoughtCo. 2018
4. *Open Up.* HM Parliament. 2015
5. John Penrose. *UK Government Response: Full Text*. WebRoots Democracy. 2016