

Punchscan

Paper-based voting with E2E auditing capabilities

Michael Senn

2022-12-07

Faculty of Science, University of Bern

Motivation

To provide a voting system, where:

- The vote is managed by a central election authority
- And voters get a paper-based receipt
- Which does not allow votes to be bought nor coerced
- Yet allows them to verify their votes are cast-as-intended
- And auditors provide resilience against a malicious EA

Ballot layout

Ballot layout

- Ballot consists of two pages, stacked on top of each other
- Both pages have serial number identifying ballot

<div data-bbox="532 322 642 381">ID: 007</div> <p data-bbox="375 405 584 453">What is your favourite prime?</p> <p data-bbox="375 477 458 550">a) 2 b) 3 c) 65535</p> <div data-bbox="334 629 625 708"><input type="radio"/> <input type="radio"/> <input type="radio"/></div>	<div data-bbox="943 322 1053 381">ID: 007</div> <div data-bbox="742 629 1033 708"><input type="radio"/> a <input type="radio"/> b <input type="radio"/> c</div>
--	---

Figure 1: Top (left) and bottom (right) halves of ballot

Ballot layout: Top page

- Top page has question and answers, mapped to symbols (here: letters)
- This mapping is randomized per ballot
- Circular cutouts allow seeing bottom page


ID: 007
<p data-bbox="573 498 797 552">What is your favourite prime?</p> <p data-bbox="573 576 659 655">a) 2 b) 3 c) 65535</p> <div data-bbox="529 738 841 824"></div>

Figure 2: Top half of ballot

Ballot layout: Bottom page

- Bottom page has answer symbols (here: letters)
- Order of these is randomized per ballot
- Symbols can be seen through cutouts in top page

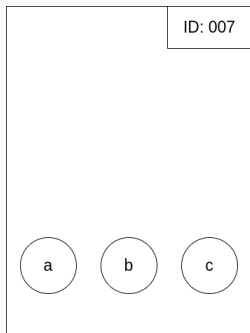


Figure 3: Bottom half of ballot

Voting process

Voting process: Voting

- Voter receives ballot, both pages stacked atop each other
- Voter marks their choice using a dauber (huge highlighter)
- This leaves stain on both top and bottom page

ID: 007
What is your favourite prime?
a) 2 b) 3 c) 65535
<div><div>a</div><div>b</div><div>c</div></div>

Figure 4: Ballot after voting

Voting process: Scanning

- Voter destroys one half of the ballot
- Other half gets scanned, and kept by voter as receipt
- Unable to learn vote by looking at one half only
- But: What to do in tally phase?

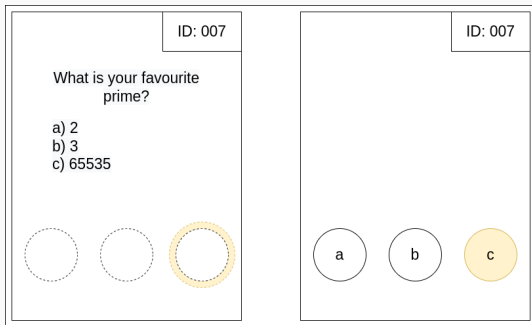


Figure 5: Top (left) and bottom (right) halves of ballot after voting

References

References

- [FCS06] Kevin Fisher, Richard Carback, and Alan T. Sherman. *Punchscan: Introduction and System Definition of a High-Integrity Election System*. May 2006. URL: <https://mdsoar.org/handle/11603/12945>.

- [Kel+10] John Kelsey et al. “Attacking Paper-Based E2E Voting Systems”. In: *Towards Trustworthy Elections*. Ed. by David Chaum et al. Red. by David Hutchison et al. Vol. 6000. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 370–387. ISBN: 978-3-642-12979-7 978-3-642-12980-3. DOI: 10.1007/978-3-642-12980-3_23. URL: http://link.springer.com/10.1007/978-3-642-12980-3_23 (visited on 11/22/2022).

- [MN10] Tal Moran and Moni Naor. “Split-Ballot Voting: Everlasting Privacy with Distributed Trust”. In: *ACM Transactions on Information and System Security* 13.2 (Feb. 2010), pp. 1–43. ISSN: 1094-9224, 1557-7406. DOI: [10.1145/1698750.1698756](https://doi.org/10.1145/1698750.1698756). URL: <https://dl.acm.org/doi/10.1145/1698750.1698756> (visited on 11/22/2022).

- [PH10] Stefan Popoveniuc and Ben Hosp. “An Introduction to PunchScan”. In: *Towards Trustworthy Elections*. Ed. by David Chaum et al. Red. by David Hutchison et al. Vol. 6000. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 242–259. ISBN: 978-3-642-12979-7 978-3-642-12980-3. DOI: 10.1007/978-3-642-12980-3_15. URL: http://link.springer.com/10.1007/978-3-642-12980-3_15 (visited on 11/21/2022).

- [Lun+12] D Lundin et al. “Tear and Destroy: Chain Voting and Destruction Problems Shared by Prêt à Voter and Punchscan and a Solution Using Visual Encryption”. In: IAVoSS Workshop on Frontiers in Electronic Elections. 2012. URL: <https://openresearch.surrey.ac.uk/esploro/outputs/conferencePresentation/Tear-and-Destroy-Chain-voting-and/99515081502346#file-1>.