Demo: Audiotegrity Voting Protocol

Richard Carback
University of Maryland, Baltimore County

Alex Florescu, Tyler Kaczmarek, Jan Rubio
The George Washington University
tkacz3t@gwmail.gwu.edu

Noel Runyan
Personal Data Systems

Poorvi L. Vora, John Wittrock
The George Washington University

Filip Zagórski
Wroclaw University of Technology

1. INTRODUCTION

End-to-end independently-verifiable voting protocols (also known as E2E protocols) enable voters to independently determine whether an election outcome is correct, without requiring them to trust election officials or voting machines. *Audiotegrity* is an electronic E2E protocol and corresponding audio ballot-casting interface used in the 2011 municipal election at Takoma Park. We propose to demo the audio interface and briefly describe the protocol. Note that the *Audiotegrity* research project is work in progress; we will also describe what parts are incomplete and can be improved.

The City of Takoma Park held the world's first E2E secret ballot public election in 2009 [3] using voting system Scantegrity. The election used paper ballots, however, and voters unable to handle paper ballots voted with human assistance, as they had in the previous local election. This motivated the development of *Audiotegrity*, which was deployed in the next local election in Takoma Park, in 2011 — the first public end-to-end election where voters with visual disabilities could cast a secret ballot.

E2E voting systems are based on cryptographic protocols that provide evidence of tally-correctness. While E2E voting systems can, and should, be tested for security vulnerabilities, it is impossible to guarantee the absence of vulnerabilities. Hence, E2E systems provide a digital audit trail which voters and observers can check to determine, with high probability, if an undetected vulnerability was used to change an election outcome. Thus the focus is not on the security of the system, which cannot be guaranteed, but on the correctness of a particular election, which can be ascertained with very high probability. E2E systems provide (new) tally-correctness evidence for *each* election, and *each* election is checked for correctness. The audit trail and checks should not reveal any information on individual votes beyond that revealed by the tally. The cryptographic checks cannot prevent fraud, but detect it with high probability.

2. PROTOCOL OUTLINE

Our protocol is a slightly-modified version of Scantegrity, used by Takoma Park in 2009 and 2011, and eTegrity, developed by us last year. For reasons of space we do not describe Scantegrity or eTegrity separately.

The following list details the *Audiotegrity* ballot-casting process for an arbitrary voter. Note that the voting system posts parts of the digital audit trail on the election website a few days before the election.

1. *Voter Arrives:* Voter is escorted to the station and assisted in putting on a headset. They will enter responses to audio prompts by pressing on a keypad.
2. *Set Preferences:* Voter sets their preferences for text size, audio speed and volume.
3. *Make Selections:* Voter makes selections.
4. *Confirm Selections:* Voter confirms their selections.Their Scantegrity confirmation numbers are read out to them.

The confirmation numbers are chosen pseudo-randomly per ballot and per candidate, before the election. The correspondence between candidates and confirmation numbers is committed to before the election, as is also the sorted list of confirmation numbers by ballot number. Commitments are published on the web-site before the election. Voters do not need to know this information if they choose not to. The commitments form part of the digital audit trail.

5. *Ballot Printed:* Station prints out an appropriately-marked ballot and ballot receipt. The ballot and ballot receipt are of distinct sizes so the voter may tell the difference.

The receipt lists the ballot ID and the confirmation numbers for each choice. The voter takes it home with them; the confirmation numbers reveal nothing about their vote.

The marked Audiotegrity ballot is meant to look identical to a Scantegrity ballot hand-marked by a voter. Both look like marked optical scan ballots, with a difference: the marked ovals bear, in a light color, the confirmation numbers corresponding to the votes. In an unmarked Scantegrity ballot, the confirmation number is printed in invisible ink in the oval. It is revealed when the voter marks the oval with a special pen. In an Audiotegrity ballot, the number is printed with the rest of the ballot by the station printer. We attempted to match the colors of the marked ovals and the confirmation codes on both types of ballots so that they would be difficult to distinguish on casual, distant examination.

6. *Cast or Audit:* Voter decides whether to cast or audit the ballot. If they cast the ballot, it is treated the same as any other ballot (the printer prints ballots face down, the voter is escorted to the scanner to cast it). If they audit it, an election official helps them make a copy of the ballot (with confirmation numbers) to take home with them and sets up the machine so they may vote again.They cannot cast an

audited ballot because the correspondence between confirmation numbers and candidates is made public in an audited ballot (see below). *This feature was not made available to all voters at Takoma Park, though an election observer audited ballots on the interface, and candidate representatives were also encouraged to do so.* It is anticipated that, as Takoma Park voters become more familiar with E2E elections, it will be easier to introduce the possibility of an audit by any voter.

7. *Voter Leaves:* Voter leaves, with a ballot receipt corresponding to their single cast ballot and any ballot copies of audited ballots.

After the election, the system publishes the following on the election website: (a) all voted ballot IDs and corresponding voted confirmation numbers (without corresponding candidates); (b) all audited ballot IDs with the correspondence between candidates and confirmation numbers; (c) the tally and that part of the digital audit trail required for tally-correctness audits.

The voter may check the confirmation numbers on their receipt and copies of audited ballots with those on the election website. Currently, a voter with visual disabilities can have a trusted friend check, without in any way revealing their vote. In a complete system, the voter would be able to check this using a simple audio interface; we discuss the challenges in the next section. Note that a voter who does not care to verify may simply ignore this step.

The voter may also check opened commitments and the outcome of the tally correctness audits. These checks are performed using software written by the voter or anyone else.

3. DISCUSSION AND FUTURE WORK

In a typical use scenario, a voter with a visual disability may use an electronic interface to obtain a representation of the same information in audio form. The trust model requires that the user trust the interface to correctly perform the transformation. In our problem, the voting system is not trusted and provides the interface. Additionally, the untrusted interface performs an action on behalf of the voter — it marks the ballot. For this reason, we rely on sighted voters using the same interface to detect ballot-marking errors. If we may assume that the interface is not able to differentiate between voters with and without visual disabilities, it would not be able to predict when it could change the vote without being caught. Note that this assumption is not always satisfied. Note also that the voter cannot bring in their own electronic ballot-marking device as it can be examined at a later time to determine how they voted.

It would be great to have an audio bulletin board accessible by phone. A voter would call the board and it would read out confirmation numbers. The challenge, e, is that the bulletin board could present one confirmation number to the voters who call in and another to the auditor who checks the tally. Future work could have the voter use a smart phone which will also check digital signatures (the phone would have to be trusted by the voter), and to somehow communicate this signed data to the auditor.

The current user interface limits the number of candidate choices. It would also need to be modified to incorporate dual-switch interfaces. This requires significant redesign.

4. RELATED WORK

E2E voting system Helios [1] is meant for use in remote-voting scenarios. Its fully electronic nature allows for the possibility of fitting an accessible interface. However, because the communication tape between the voter and Helios is essentially owned by the computer and is not write-once, nor visible to the voter, the computer may claim the vote was for Bob, while it may have been for Alice. While the voter knows that the computer or Helios cheated, they have no way of proving it, nor of knowing which of the two cheated. Audiotegrity might appear to have a similar problem — a sighted voter can determine that the ballot was incorrectly marked but cannot prove it. However, in Audiotegrity, all sighted voters can detect this issue, whenever it is attempted. A Helios voter determines an attempt to change their vote only if they choose to audit the ballot. If the Audiotegrity interface is not caught incorrectly marking ballots, any attempts by it to attribute incorrect confirmation numbers (swapping them, say) to change a vote will be detected with high probability if many voters audit their votes.

5. USE OF THE INTERFACE

We performed preliminary usability tests on a population of users who responded to an announcement by the City of Takoma Park. The tests revealed some issues with the instructions and features, some of which we were able to address before the election.

The interface was used by both sighted and unsighted voters in the election of 2011, though a vast majority of the votes were cast by directly marking paper ballots. Audiotegrity was acknowledged as a valuable contribution by the Chair of the Board of Elections and a sitting City Council member in the televised and video recorded election certification meeting.

6. ACKNOWLEDGEMENTS

This research was supported in part by NSF Award Nos. 0831149 and 0937267 and by Research Enhancement for Undergraduates (REU) scholarships from these awards. The Board of Elections and the City Clerk of Takoma Park were very generous with their time and knowledge of electoral practices and voter behavior. Assistant City Clerk, Irma Andia, translated English script into Spanish and read most of the audio. The Communications Department of the city provided the audio recording.

7. REFERENCES

[1] Ben Adida. Helios: Web-based Open-Audit Voting. In *Proceedings of the Seventeenth Usenix Security Symposium (USENIX Security 2008)*, June 2008.

[2] David Chaum et al. Scantegrity II: End-to-end verifiability for optical scan election systems using invisible ink confirmation codes. In *EVT'07: Proceedings of the USENIX/Accurate Electronic Voting Technology on USENIX/Accurate Electronic Voting Technology Workshop*. USENIX Association, 2008.

[3] Richard Carback et al. Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy. In *Proceedings of the Ninteenth Usenix Security Symposium (USENIX Security 2010)*, August 2010.