Dispute Resolution in Accessible Voting Systems: The Design and Use of Audiotegrity

Tyler Kaczmarek[1], John Wittrock[1], Richard Carback[2], Alex Florescu[1], Jan Rubio[1], Noel Runyan[3], Poorvi L. Vora[1], and Filip Zagórski[4]

[1] Department of Computer Science, The George Washington University*
[2] Network and Information Concepts Group, Charles Stark Draper Laboratories
[3] Personal Data Systems
[4] Institute of Mathematics and Computer Science,
Wroclaw University of Technology**

Abstract. We describe in detail dispute resolution problems with cryptographic voting systems that do not produce a paper record of the unencrypted vote. With these in mind, we describe the design and use of Audiotegrity—a cryptographic voting protocol and corresponding voting system with some of the accessibility benefits of fully-electronic voting systems and some of the dispute resolution properties of paper-ballot-based systems. We also describe subtle issues with coercion-resistance if accessible systems are not well-designed.

Audiotegrity was designed in response to a request by Takoma Park election officials, tested in a public test organized by the city in June 2011, and used in its municipal election in November 2011. We are not aware of any other precinct-based end-to-end independently-verifiable election for public office where the protocol enabled participation by voters with visual disabilities.

Keywords: end-to-end voting systems, accessible, dispute resolution.

1 Introduction

Several cryptographic voting protocols have been proposed for polling place elections, where voters use voting systems that they do not trust. Many of the corresponding voting systems use paper ballots (Prêt à Voter [20,10], Scantegrity II [8]) scanned after the voter marks her choice(s). Paper ballots are severely limiting from a usability and accessibility perspective. On the other hand, the straightforward replacement of interactions on paper with similar interactions

* This work was supported in part by NSF Award Nos. 0831149, 0937267 and 1137973 and by Research Experience for Undergraduates (REU) enhancements to these awards. It was determined to be Exempt, Category 2—GW IRB application 061109.

** This research was partially supported by NCN scientific project 2010-2013 - grant number N N206 369839.

J. Heather, S. Schneider, and V. Teague (Eds.): VoteID 2013, LNCS 7985, pp. 127–141, 2013.

over an electronic medium does not always preserve a protocol's security properties. This paper makes the following contributions. First, it describes in detail the dispute resolution weaknesses of voting systems where voters do not manually mark ballots. Second, it presents the design and deployment of Audiotegrity, a protocol and corresponding voting system, that seeks a balance between the strong accessibility and usability properties of fully-electronic voting systems and the strong dispute resolution properties of paper-ballot-based ones. Audiotegrity was used by the city of Takoma Park for its municipal election in November 2011.

Audiotegrity provides an electronic interface for the voter to enter a vote, and produces a marked Scantegrity II ballot which is then scanned and processed in the same manner as a hand-marked paper Scantegrity II ballot. From the available descriptions, the version of Prêt à Voter proposed for use in Victoria [6] and STAR-Vote [4] use similar interfaces. The focus of this paper is twofold. First, it presents the security implications of the use of paper vs. electronic interactions in various protocol steps. Second, it describes the design of a protocol that takes these into consideration, and the use of the corresponding system in tests in June 2011 and a real election in November 2011. In particular, we observe that paper ballots or ballot summaries play a role not only in manual recounts, but in the protocol itself, even when the voting system is a good cryptographic system. Paper and physical procedures enable some aspects of dispute resolution and coercion-resistance for human voters, who are not able to make and check digital commitments and signatures in the polling booth.

We note at the outset that we focused on the vote-casting experience. We did not implement interfaces for voters to interact with the website that displays confirmation numbers and audit information. However, voters can use accessible devices, in general, for electronic information displayed on appropriately-designed websites. Voters cannot use personal accessible devices while voting, as such a device would learn the vote.

In section 2 we provide background, and in section 3 we describe related work. In 4 we describe the dispute resolution and coercion-resistance problems with voting systems that do not show the voter a paper record of her unencrypted vote. In section 5 we describe the Audiotegrity protocol and its security properties. In section 6 we describe the dispute resolution and coercion-resistance properties of paper-ballot protocols Prêt à Voter and Scantegrity II and compare them with those of Audiotegrity. In section 7 we describe the use of Audiotegrity in Takoma Park in 2011. We conclude in section 8.

2 Background

In the typical cryptographic voting protocol, each vote is encrypted and all encrypted votes are broadcast on an election website. Voters may treat encrypted votes as receipts and take them home to check that they are correctly broadcast. Encrypted votes are processed in a verifiable manner to obtain the tally.

Vote Encryption: We will focus on precinct-based protocols—where the voter votes from a polling booth, and the cast/audit paradigm proposed by Benaloh [3].

Some protocols use specially-designed paper ballots with the property that a voter can encrypt her vote simply by filling the ballot, see Figure 1.

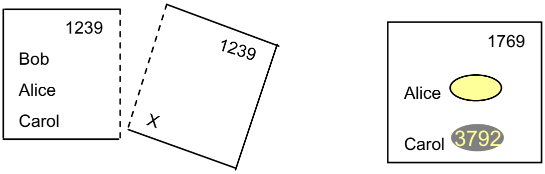

Fig. 1. Marked ballots: Left: *Prêt à Voter* Right: *Scantegrity II*

For example, Prêt à Voter ballots list the candidates in a pseudo-random permutation on the left side of the ballot. The voter marks her choice on the right side and then separates the two ballot halves along a central perforation. The half with the candidate order is shredded and the marked half cast. The serial number provides the information necessary for the voting system to interpret the mark, and the position of the mark is the encryption of the vote.

For another example, the Scantegrity II voter marks ballots that are very similar to optical scan ballots, with a single important difference. Each oval has printed on it, in invisible ink, a confirmation number—the encryption corresponding to this vote choice. When voters filled the oval with a special pen, the confirmation number becomes visible. The same functionality can be achieved through the use of scratch-off surfaces.

Other protocols like Votebox and simple-verifiable voting rely on encryption machines in the polling place to perform the encryption.

Once the vote is encrypted, it is cast or audited, see Figure 2. If the encryption (i.e. the receipt) is audited, the voting system provides a proof that it encrypted the vote correctly, and the proof is public. The corresponding vote cannot be cast as the correspondence between the encryption and the vote is now public, and the vote no longer secret. The voter goes through a fresh encryption process which will again end in a cast or audit.

Voters take home copies of the final cast encryption as well as voting system responses to audits. They may check the presence of these on the election website, and the correctness proofs of the audited encryptions using software obtained from any—and, in fact, several—sources. Thus the voter need not have access to trusted software in the polling booth. The tally is computed in a verifiable manner from the encrypted votes posted on the website. After the election outcome is announced, the tally computation is publicly audited. Anyone can write software to check the audits.

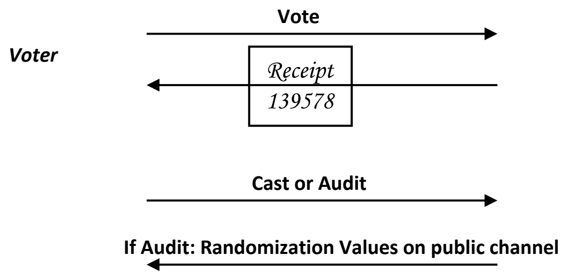

Fig. 2. The Benaloh Cast/Audit Paradigm

3 Related Work

Accessible Interfaces for Voters: The Voting-on-Paper Assistive Device (Vote-PAD) [1] enables voters with visual or dexterity impairments to complete paper ballots. The device consists of a plastic ballot-sleeve, tactile indicators and an audio tape recording, customized for each election and ballot design. Similar devices, called Tactile Ballots, have been used in elections in Rhode Island [13]. Prime III [12] provides a multimodal interface to a voting machine with a voter-verifiable video audit trail (VVVAT) that is a video record of all interactions with the voting machine. A preliminary proposal for accessible audio-based electronic protocols appears in [11]. These protocols, however, are not practical enough for use in real elections.

Dispute Resolution: Saltman [21] and Mercuri [19] were among the first to describe problems with voting systems not following instructions. They demonstrated these problems in non-cryptographic voting systems. We show, in section 4, that similar (though not identical) problems can persist in cryptographic voting systems. Kiayias and Yung provide a dispute-free protocol [16] in the classical cryptographic protocol model (all participants are interactive probabilistic polynomial time Turing machines) which was followed by proposals for several dispute-free protocols in the same model. We examine the problems that arise because voters are not probabilistic polynomial-time Turing machines, as proposed by Adida [2]. Küsters, Truderung and Vogt provide a rigorous definition of accountability for voting and other cryptographic protocols [18]. The definitions used is closely related to our notion of dispute resolution. The problems they identify are not, however, related to the cast/audit paradigm, nor to the use of paper. We have referred briefly to dispute resolution problems with the cast/audit paradigm in [9].

Use of Accessible Voting Systems in Real Elections: The protocol we describe in section 5 is very similar to the STAR-Vote proposal and the version of Prêt à Voter proposed for use in Victoria. Neither proposal describes how voters commit to casting or auditing ballots. The STAR-Vote proposal does not distinguish among spoiled and audited ballots and does not describe how to resolve disputes regarding whether a ballot was audited or cast. The STAR-Vote proposal also does not describe if blank paper ballots are available for voters in case the voting machine does not print the vote as directed.

4 Problems with Dispute Resolution in the Absence of Paper

We first consider a protocol that does not use paper at all: VoteBox. In this instance of the cast/audit paradigm (see figure 3), the voter enters a vote into a voting machine, which provides an encryption of the vote; this encryption is immediately published on the bulletin board. The voter then chooses whether to cast the ballot or audit it. If she chooses to audit it, the machine publishes (or provides) the randomization used in the encryption. If she chooses to cast it, the encrypted value is published among cast ballots. All communication is electronic.

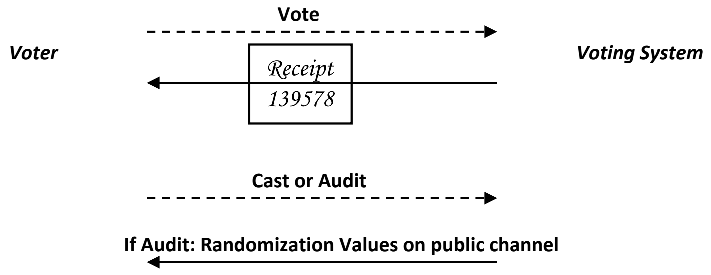

Fig. 3. The channel from voter to voting system is electronic. A dashed line shows interactions that are not verifiable by a third party and hence result in dispute resolution weaknesses.

We consider two problems with VoteBox because the machine may deviate from protocol and not follow the voter's instructions.

The voter provides two sets of instructions: the vote and whether to cast or audit. We consider each separately below.

1. **Machine encrypts a vote other than that cast:** The voter is able to detect the deviation on audit. Hence, if the machine changes a large enough number of votes in this manner, the probability of at least one voter detecting this on audit is large. However, the protocol does not enable the voter to prove such deviation. The channel from voter to voting machine is electronic and there is no record—other than that held by the voting machine—of the voter's command. Hence a third party would not be able to determine whether the voter or the voting machine was lying.
2. **Machine does not follow cast/audit instruction:** The voter is always able to detect the deviation. However, as above, the voter is not able to prove the deviation to a third party.

The reason the above deviations cannot be proven to a third party is that—in both instances—there is no record of the voter's instruction, see figure 3. The fact that the dispute cannot be resolved is an important problem. In particular, the general public cannot distinguish between (a) an incorrect election outcome and (b) a group of dishonest voters calling an honest election into question.

It has been proposed that other approaches—such as auditing a machine in public during the election—may be used to determine whether a machine is truly behaving honestly. However, as with parallel testing, such approaches are vulnerable to "cryptic knocks". An insider present at the polling location might easily warn the voting machine through a side channel that it is being audited. The channel may be implemented in various ways, including a modified election console which can send to the booth a packet that satisfies a predefined property. The channel can also be implemented using different machines working in the same sub-network (i.e. ARP packets) or by equipping the booth with an additional network (3G/WiFi/...) connection. In fact, such an attack is far simpler than the many fairly complex attacks against non-cryptographic systems described in the secure voting systems literature. Source code analysis does not help since the malicious code can be injected at the hardware level (eg. Rakshasa [5]).

We now consider the original version of the simple verifiable voting approach. It proposes that the vote encryption may be provided to the voter on paper (the receipt in figure 3 is provided on paper). The voter may then take the paper to another device to cast or audit it. Here too the two instructions from the voter—the vote and the cast/audit command—are communicated to an electronic device using an electronic interface, where the electronic device holds all records of the commands. Again, disputes between the machine and the voter such as those described above are not resolvable by a third party.

As mentioned earlier, Saltman and Mercuri both pointed out similar problems with fully-electronic non-cryptographic voting systems: the machine need not follow voter instructions. There is a major difference between the (fully-electronic) cryptographic and non-cryptographic voting systems, however: using the cryptographic voting system, a voter can catch a cheating system, even if he or she cannot prove this to others. In the non-cryptographic voting system, the voter does not know whether the system followed instructions.

The ability of the machine to ignore instructions (without the voter being able to prove this) can be used in multiple ways to change the election outcome. First, the machine can encrypt votes for a particular candidate. Second, it can choose to always encrypt the correct vote, audit it on occasion (ignoring whether the voter wanted to cast or audit) and then immediately cast one of its own choice (claiming the voter audited and then entered a vote and chose to cast it). Third, it may claim a vote was audited after a voter thought he or she had cast it. There would be many other combinations.

Note that the weaknesses we demonstrate are *not* weaknesses of the cast/audit approach which greatly simplifies the user experience. These are weaknesses resulting from the type of channel used for communication.

5 Audiotegrity

We describe only the front end of Audiotegrity, designed around the cast/audit paradigm. The back-end corresponds to the voting system used—in our case, Scantegrity II. The voter enters her votes on an electronic interface that produces a printed marked ballot and cryptographic receipt, face down. Before the voter can look at the ballot (which, in the Scantegrity II case contains the receipt value in the form of confirmation numbers), she must declare publicly, at the polling site, whether she wishes to cast or audit the ballot. This is to prevent coercion attacks, such as described in [15]. She may then check that the ballot is marked correctly and make a copy to take home if it is an audited ballot, or else cast it at the scanner.

We first describe the aspects of Scantegrity II relevant to Audiotegrity, and then describe Audiotegrity in more detail.

5.1 Scantegrity

The Scantegrity confirmation numbers are chosen—pseudo-randomly per ballot and per candidate—by the voting system before the election. Also before the election, the voting system publishes commitments to (a) the correspondence between candidates and confirmation numbers for each ballot and (b) the sorted list of confirmation numbers by ballot number. Voters do not need to know this information to cast a valid vote.

Voters who manually fill out paper Scantegrity ballots also fill out the confirmation card manually if they wish to check the numbers later, writing down confirmation numbers they see. There is nothing special about the confirmation card, which is simply provided as an aid to the voter; the voter may note these numbers on any paper or memorize if they can and wish to do so. Those who do not wish to check later may ignore the confirmation numbers.

Immediately after the election, the system publishes the following on the election website:

1. all voted ballot IDs and corresponding voted confirmation numbers (without corresponding candidates);
2. all audited ballot IDs with the correspondence between candidates and confirmation numbers;
3. the tally and that part of the digital audit trail required for tally-correctness audits.

The voter may check the confirmation numbers on her receipt and any copies of audited ballots with those on the election website. Note that a voter who does not care to verify may simply ignore this step. If a voter finds that her confirmation number is not correctly displayed on the website, she may file a dispute, declaring the number she claims should be on the website instead.

The Scantegrity scanner may be programmed to reject overvoted ballots, so that a voted ballot may not be later over-voted by an insider with access to the ballots. (This was not implemented for the election and can result in a dispute resolution problem, but is not a problem with the protocol).

After the period for filing disputes is over (generally a few days after the election), the voting system publishes all voted ballot IDs and the corresponding sorted list of all confirmation numbers. It also provides the information necessary to check the commitments to these values. All disputes by voters may be checked against this information. If, while filing the dispute, the voter provided a confirmation number that is on the list of confirmation numbers committed to for the ballot, but was not listed as a voted confirmation number, it is very likely that the voter was correct. This is because the probability that the voter would correctly guess a voted confirmation number is low. On the other hand, if the number provided by the voter is not on the list of numbers committed to by the voting system, it is unlikely that the voter is correct if ballot audits do not detect problems. Thus dispute resolution in Scantegrity, unlike that in Prêt à Voter), does not depend on digital signatures or an authenticated receipt. The receipt is not what the voter has, but what the voter knows. The purpose of a digital signature is served by the fact that the confirmation numbers on a single contest consist of a very small set of all possible confirmation numbers.

While dispute resolution in Scantegrity is probabilistic and depends on a large-enough number of ballot audits, the dispute resolution problems we identify in section 4 are not resolved by a large-enough number of audits unless we make different assumptions, such as a large enough number of honest voters (an assumption not required by paper ballot systems Scantegrity and Prêt à Voter).

5.2 Audiotegrity

The station has a privacy screen and is not visible from the voting floor. The printer attached to the station is preferably visible to the public and to poll workers, just as the scanner is (it can be outside the privacy-screened area, for example, or the privacy-screened area may be designed so that the voter may vote privately while the printer is visible).

The ballot and confirmation card are of distinct sizes so that it is easy to know the difference by touch and/or sight.

An audio record of the confirmation numbers would be useful (we currently do not provide this). We attempted to match the colors of the marked ovals and the confirmation codes on both types of ballots—the Scantegrity ballots marked manually by voters and the Audiotegrity machine-marked ballots—so that they would be difficult to distinguish on casual, distant examination.

Figure 4 provides a summary of Audiotegrity as a cast/audit protocol, and figure 5 an illustration of the voting process. We follow this with a more detailed description of the protocol.

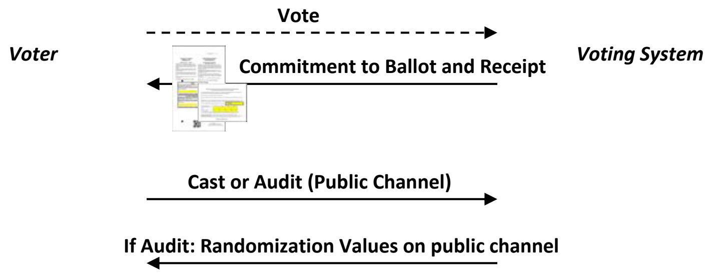
Vote
Voter
Commitment to Ballot and Receipt
Voting System
Cast or Audit (Public Channel)
If Audit: Randomization Values on public channel

Fig. 4. A summary of the Audiotegrity voting protocol. A dashed line shows interactions that are not verifiable by a third party and hence result in dispute resolution weaknesses.

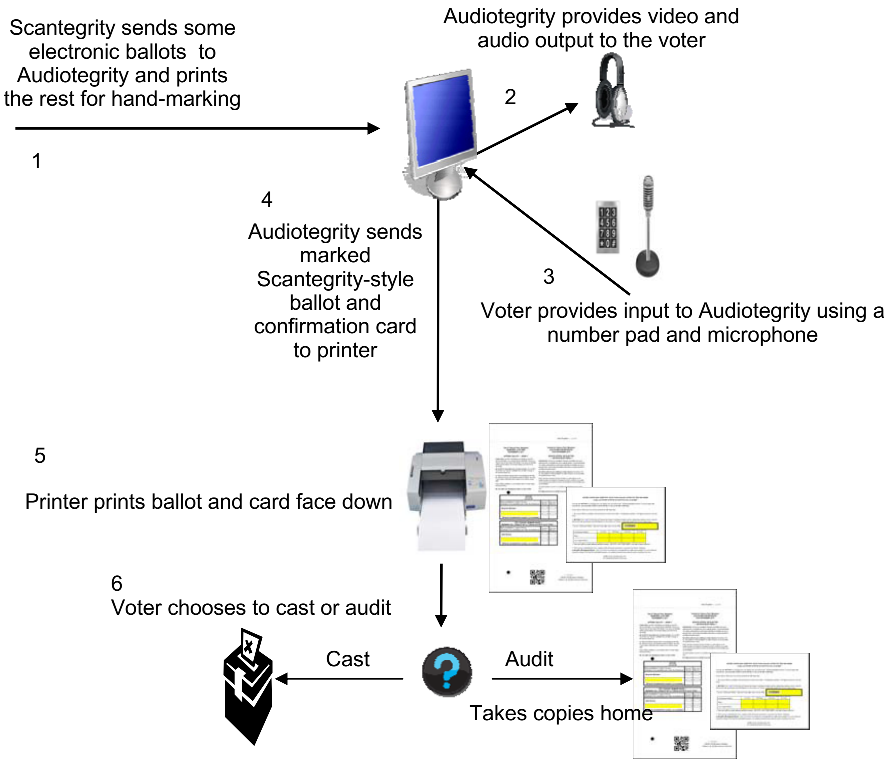
Scantegrity sends some electronic ballots to Audiotegrity and prints the rest for hand-marking
1
Audiotegrity provides video and audio output to the voter
2
3
Voter provides input to Audiotegrity using a number pad and microphone
4
Audiotegrity sends marked Scantegrity-style ballot and confirmation card to printer
5
Printer prints ballot and card face down
6
Voter chooses to cast or audit
Cast
Audit
Takes copies home

Fig. 5. The Audiotegrity Voting Protocol

Audiotegrity Ballot Casting Protocol

1. *Voter is Authenticated:* The voter is authenticated for voting by the physical process used by the jurisdiction.
2. *Voter Arrives at Station:* The voter is escorted to the station. The voter is assisted in putting on a headset. The location of the keypad designated for input and the printer that will output the ballot is described to the voter, and the voter's Ward number is input to the voting machine.
3. *Set Preferences:* The voter sets her preferences for audio speed and volume (and optionally for text size).
4. *Make Selections:* The voter makes selections. She can record a speak-in choice, which is later interpreted by election officials (write-in votes on Scantegrity ballots are also interpreted by election officials).
5. *Confirm Selections:* The voter confirms her selections.
6. *Ballot Printed:* The voting station prints out face-down:
   - **ballot** an appropriately-marked Scantegrity ballot with Scantegrity confirmation numbers printed in the ovals next to the chosen candidate(s).
   - **confirmation card** a Scantegrity confirmation card which lists the ballot ID and the confirmation numbers for each choice. The voter takes the card home with her; the confirmation numbers reveal nothing about the vote.
7. *Cast or Audit:* Before the voter leaves the station, touches the ballot or identifies any information on it, the voter decides whether to cast or audit the ballot and publicly informs a poll worker of her decision. (Note that if the voter decides to cast or audit her ballot after seeing the confirmation numbers, the protocol is vulnerable to the coercion attack of [15].)

   If the ballot is:

   cast it is treated the same as any other ballot:

   (a) the voter looks at it and checks that it is correctly marked,
   (b) the voter checks that the confirmation card lists the correct confirmation numbers or makes a separate note if she desires,
   (c) the voter is then directed to the scanner where the ballot is cast and scanned in.

   The voter with visual disability is protected by other voters using the same station and detecting printing errors.

   The sighted voter may notice that the ballot is not marked correctly. In the event that this happens, the voter may choose to spoil the ballot and restart the voting process from the head of the line. Spoiled ballots are not treated the same as audited ballots. As with the Scantegrity voting system, spoiled ballots are not revisited.

   audited an election official helps the voter make a copy of the ballot (with confirmation numbers) to take home with her and sets up the machine so she may vote again.

   Both the original audited ballot and the copy bear signatures of both: the voter and the election official. The voter cannot cast an audited ballot because the correspondence between confirmation numbers and candidates is made public in an audited ballot.
8. *Voter Leaves:* The voter leaves, with a ballot receipt corresponding to her single cast ballot and any ballot copies of audited ballots.

5.3 Properties

Note that if the system provides wrong confirmation numbers for the voter's choice of candidate, it is caught during an audit. The voter can prove that the system provided the wrong confirmation number, because her vote is marked on the ballot. If the voting system posts a number online that the voter claims is incorrect, this can be resolved as with Scantegrity, described in section 5.1.

The voting system can mark the wrong candidate on the ballot. This will be detected every time a ballot is marked incorrectly and not only during an audit; however, the voter will not be able to prove that the machine marked the wrong candidate. This is because the channel between the voter and the voting machine is electronic, and all records are held by the voting machine. The voter may spoil the incorrectly-marked ballot and vote again. Because information on spoiled ballots is not made public, this does not introduce a coercion threat.

The proof of incorrect printing is not transferable, and each voter must convince his or herself that the printer is printing correctly. This aspect can, however, be checked without special effort by sighted voters. Voters with visual disability can avail of independent verification provided at the polling place (as defined by the Voluntary Voting Systems Guidelines 1.1 [22, section 7.8]). (We were not able to provide this for the 2011 election). However, because the independent verification is not guaranteed to be independent, voters with visual disability also rely on others using the same stations, and on the system itself not being able to tell the difference between voters. Because personal electronic ballot readers would know the correspondence between vote and confirmation number, voters cannot use these to read unaudited ballots. It would be difficult to monitor and enforce the use of personal readers only on audited ballots. When there is no complaint of incorrect printing, voters with visual disability can rely on the printers printing correctly.

The Audiotegrity audit checks only a single correspondence between candidate and confirmation number for each choice, unlike the Scantegrity II audit which checks all confirmation numbers on the ballot. This does not appear to result in any coercion or integrity related problems.

The machine knows the codes for all Audiotegrity ballots, and no others. Its knowledge of codes is no different from that of the printer for Prêt à Voter or Scantegrity II.

Finally, unlike fully-electronic protocols, this protocol is not "fully-accessible". A voter might need assistance to take the filled-in ballot to the scanner.

6 Comparison of Protocol Properties

We now provide a comparison of the properties of Scantegrity II, Audiotegrity, simple verifiable voting and voting by DRE.

Suppose a cheating Scantegrity II voting system provides incorrect confirmation numbers. This is caught through a ballot audit, and there is never an unresolved dispute that it is cheating in this manner. That is, the proof of cheating is transferable to another voter, and one voter checking helps other voters too.

A cheating Audiotegrity voting system can:
(a) mark the wrong oval (with the confirmation number corresponding to this oval; that is, cast a valid vote for a candidate other than the voter's choice). This is caught without an audit — i.e. it is almost always caught. However, a dispute cannot be resolved and proof of it cheating in this manner is not transferable. Because a voter catches the cheating, she can vote again, including with a paper ballot. This is an unresolved issue for voters with visual disability (in any voting system, to our knowledge).
(b) mark the correct oval with the wrong confirmation number. This is caught in the manner of Scantegrity II, and the dispute is resolvable. The proof of cheating is transferable.

A cheating system based on simple verifiable voting can
(a) print a valid encryption of an incorrect vote, in the manner of the first Audiotegrity attack (a). The system is detected to be cheating by the voter only on audit. A dispute between voter and system—each claiming to be correct—is not resolvable and the proof is not transferable. Repeated instances can prevent a voter from voting. While many complaining voters can draw attention to this problem, the absence of paper ballots means there is no other way to vote. Additionally, a small group of voters can call an honest election into unresolvable dispute. Finally, this is detected by the voter only on audit, so many valid incorrect votes may be cast.
(b) print an invalid encryption, similar to the second Audiotegrity attack (b). This is caught on audit and the dispute is resolvable.

A cheating DRE need not reveal it is cheating, and hence will not be caught cheating as it provides no information about the election.

Voting systems that maintain paper trails such as Scantegrity II and STAR-Vote are vulnerable to coercion from insiders with access to the paper trail, as a voter's ballot ID reveals her entire vote.A level of indirection can be provided through distinct serial numbers and online verification numbers (with a correspondence protected by a shared secret), with the latter being torn off before the ballot is cast (this, again provides a usability challenge) such as described for Scantegrity II [8]. Prêt à Voter, where one half of the ballot is destroyed after the ballot is marked, does not maintain a paper trail. However, the printer that prints Prêt à Voter ballots before the election, or the machine that prints a marked ballot in the proposed solution for elections in Victoria, does know the vote too. Perhaps Prêt à Voter ballots can be printed using the independent-ballot-sheet approach of Punchscan [14]. Clearly, voting systems that do not maintain paper trails cannot carry out statistical manual audits through hand counting of paper ballots.

7 Audiotegrity in Takoma Park

The City of Takoma Park neighbors the city of Washington DC and has a population of about 17,000 with about 10,000 registered voters. The turnout in municipal elections is about 15-25%. In municipal elections, the city elects a mayor and six council members and ballots can also list referendums. Each contest has a write-in option. Takoma Park uses instant-runoff voting, and voters may rank candidates. Ballots are in English and Spanish. There was a single precinct for the 2011 election.

Both city officials and the voting population had experience with cryptographic voting systems as the city had used Scantegrity II in their 2009 municipal election [7]. Election officials wished to use Scantegrity II in 2011 too, but also wished to provide a more accessible alternative. In previous municipal elections that used optical scan technology (including the 2009 election) voters with difficulties handling paper ballots had voted with assistance. We began the design of the system in early 2011, when approached by the Board, and provided demonstrations of prototypes in a couple of election board meetings in the first half of 2011. We received no compensation from Takoma Park for its use of Audiotegrity.

The city of Takoma Park held an open test of Audiotegrity on June 8, 2011 in the Takoma Park Community Center. The test was publicized in the local news media and election officials sent announcements to various special-interest listservs. The test was not restricted to Takoma Park residents, and all who were interested were allowed to test the system. About 25-30 individuals tested the system and about 24 individuals filled out a survey. The purpose of the survey was not usability research, but to obtain feedback on the system in an informal manner, and to make potential users of the interface aware that Takoma Park might choose to use it in the election. A remote voting system was tested at the same time and place. Because we collected the data informally and interacted considerably with participants while they were testing the system, and the number of participants was very small, we do not present the data from our surveys. To obtain a qualitative, independent, albeit brief, assessment of the test, the reader may refer to a blog article [17, last paragraph].

We made some changes based on the criticisms and concerns of some participants: we provided variable speed and volume for the audio and obtained a professional recording for the real election. We also changed the instructions to make them more understandable.

The Audiotegrity system was deployed on November 8, 2011, as an accessible interface to be used alongside Scantegrity II. The protocol used in Takoma Park was different from that described in section 5.2 in a few aspects. No public declaration was required to cast or audit, and the ability to audit the ballot was not publicized widely. This was to simplify the process for the first use of the system. We chose to give audio confirmation codes to the voter before the printing began. Again, this was a consequence of the fact that we were not planning on many voter audits in this election and we wanted to provide voters with visual disability some of the information that sighted voters got. A better way to do this would be to provide digital media with confirmation codes on it.

Audiotegrity was used to cast a few votes including by poll workers and auditors. Audits were made on the system by the election auditor, Neal McBurnett. This election marks one of the first times (if not the first) where the voting system design did not prevent a voter with visual disability from independently casting an E2E ballot in a secret ballot precinct-based public election.

We are not able to provide information on how Audiotegrity votes were audited. We consciously do not keep information on Audiotegrity ballot IDs after the election, in order to reduce the ability to distinguish between Audiotegrity and Scantegrity ballots.

At the election certification meeting, Audiotegrity was called out as a valuable contribution by the chair of the board of elections and a council member.

8 Conclusions

In conclusion, what appear to be small details play an important role in protocol security. Cryptographic protocols assume secure authenticated channels between probabilistic-polynomial-time Turing machine participants. Real elections involve human voters who cannot compute signatures or commitments. Paper plays a role in providing authenticated communication between the voter and the untrusted voting machine. Additional, small changes in procedures can make a difference to security properties. We designed Audiotegrity with these issues in mind. It was used by the City of Takoma Park in its 2011 city election.

Acknowledgements. 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. Veronica Elsea of Laurel Creek Music shared with us her considerable expertise in audio recording. Neal McBurnett audited ballots.

References

1. Accessible voting without computers, `http://www.vote-pad.us/`
2. Adida, B.: Advances in Cryptographic Voting Systems. PhD thesis. MIT (2006)
3. Benaloh, J.: Simple verifiable elections. In: EVT (2006)
4. Benaloh, J., Byrne, M., Kortum, P.T., McBurnett, N., Pereira, O., Stark, P.B., Wallach, D.S.: STAR-Vote: A secure, transparent, auditable, and reliable voting system. CoRR, abs/1211.1904 (2012)
5. Brossard, J.: Hardware backdooring is practical. In: DEFCON (2012)
6. Burton, C., Culnane, C., Heather, J., Peacock, T., Ryan, P.Y.A., Schneider, S., Teague, V., Wen, R., Xia, Z.(J.), Srinivasan, S.: Using Pret a Voter in Victoria State Elections. In: EVT/WOTE (2012)
7. Carback, R., Chaum, D., Clark, J., Essex, A., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., Sherman, A.T., Vora, P.L.: Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy. In: USENIX Security Symposium (2010)

8. Chaum, D., Carback, R., Clark, J., Essex, A., Popoveniuc, S., Rivest, R.L., Ryan, P.Y.A., Shen, E., Sherman, A.T., Vora, P.L.: Scantegrity II: end-to-end verifiability by voters of optical scan elections through confirmation codes. IEEE Transactions on Information Forensics and Security 4(4), 611–627 (2009)
9. Chaum, D., Florescu, A., Nandi, M., Popoveniuc, S., Rubio, J., Vora, P.L., Zagórski, F.: Paperless independently-verifiable voting. In: Kiayias, A., Lipmaa, H. (eds.) VoteID 2011. LNCS, vol. 7187, pp. 140–157. Springer, Heidelberg (2012)
10. Chaum, D., Ryan, P.Y.A., Schneider, S.: A practical voter-verifiable election scheme. In: De Capitani di Vimercati, S., Syverson, P.F., Gollmann, D. (eds.) ESORICS 2005. LNCS, vol. 3679, pp. 118–139. Springer, Heidelberg (2005)
11. Popoveniuc, S., Chaum, D., Hosp, B., Vora, P.L.: Accessible voter verifiability. Cryptologia 33(3), 283–291 (2009)
12. Vincent Cross II, E., McMillian, Y., Gupta, P., Williams, P., Nobles, K., Gilbert, J.E.: Prime III: a user centered voting system. In: CHI 2007 Extended Abstracts on Human Factors in Computing Systems (2007)
13. Fresolone, M.: Tactile ballots alternative voting method for the blind, `http://www.votersunite.org/info/tactileballots.asp`
14. Carback III, R.T., Popoveniuc, S., Sherman, A.T., Chaum, D.: Punchscan with independent ballot sheets: Simplifying ballot printing and distribution with independently selected ballot halves. In: WOTE (2007)
15. Kelsey, J., Regenscheid, A., Moran, T., Chaum, D.: Attacking paper-based E2E voting systems. In: Chaum, D., Jakobsson, M., Rivest, R.L., Ryan, P.Y.A., Benaloh, J., Kutylowski, M., Adida, B. (eds.) Towards Trustworthy Elections. LNCS, vol. 6000, pp. 370–387. Springer, Heidelberg (2010)
16. Kiayias, A., Yung, M.: Self-tallying elections and perfect ballot secrecy. In: Naccache, D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 141–158. Springer, Heidelberg (2002)
17. Kiser, M.: Internet voting 2.0 and other advances in election technology in takoma park. FairVote Blog (June 9, 2011)
18. Küsters, R., Truderung, T., Vogt, A.: Accountability: Definition and Relationship to Verifiability. In: ACM CCS (2010)
19. Mercuri, R.: Electronic Vote Tabulation Checks and Balances. PhD thesis, University of Pennsylvania, Philadelphia, PA (October 2000)
20. Ryan, P.Y.A.: A variant of the Chaum voter-verifiable scheme. Technical Report 864, School of Computing Science, University of Newcastle upon Tyne (2004)
21. Saltman, R.G.: Effective use of computer technology in vote-tallying. Technical report, NIST (1975)
22. Technical Guidelines Development Committee, Election Assistance Commission. Voluntary voting system guidelines 1.1 (2007), `http://www.eac.gov/assets/1/AssetManager/VVSG_Version_1-1_Volume_1_-_20090527.pdf`