Electronic Voting Systems
Is Brazil ahead of its time?

Pedro A. D. Rezende
Department of Computer Science - University of Brasilia

Abstract

We describe the limited deployment of verifiable voting electronic mechanisms in Brazil, along with the corresponding political and public reactions. In particular, we discuss how the use of such voting machines may be impacted by a long-held Brazilian tradition of corruption and electoral fraud. Our observations may prove valuable in the context that systems similar to that in Brazil are under consideration in several other countries with similar political climates.

1 Introduction

In May 2001, the president of the Brazilian Senate publicly admitted to spying on secret voting on the Senate floor [1] using an allegedly intentional back door in the electronic voting system used in senate. The resulting scandal – fueled by the fact that public elections are conducted using similar electronic devices – resulted in his resignation. It also set the climate for the approval of legislation requiring such devices to be made *voter-verifiable* (or *vv*), meaning that the voter can check that his vote was received and tallied [2]. This was done by the addition of a printer to the voting machines, which are known as *Direct Recording Electronic* (or *DRE*) machines. After the voter has input his choices, these would be printed on a slip of paper, and shown to the voter. In order not to simplify vote selling, this slip of paper is not given to the voter, but displayed behind a window. After the voter has approved the vote, it is counted, and the slip of paper transferred to a sealed bag.

The most prominent feature of current *DRE* voting machines is their inability to allow for recounts, as they do not not record individual votes, but only the sums per candidate per precinct. Therefore, apart from allowing the voter to verify that his vote was correctly received, the *vv* system would have the additional feature of allowing recounts using the paper slips. Recounts would allow for the detection of potential errors in precinct sums caused by malicious tweaking with the software; such modifications would otherwise not be detectable, given the ineffective auditing of the *DRE* software.

Sadly, Brazil has had a pattern of electoral fraud, and many political careers have benefited from being able to manipulate ballot boxes [7]. With its current electronic system and electoral process, fraud can be done invisiblely by insiders and, while the system is generally believed to be secure, unsuspectedly as well. And even more sadly, general naiveness with technology may be contributing to harden that pattern. A current indication of such hardening can be traced to the well-respected Gallup institute. Gallup performs polls worldwide, including election polls – but not election polls in Brazil. Huge disparities inbetween competing polls, and between final polls and outcomes from an opaque electoral system believed to be reliable,

may explain: It is not beneficial to let one's reputation of being a reliable poller be muddied by notable, intriguing disparities. Note that if an unsuspected insider scheme to defraud an election ensues, or a set of them compete, scientific polls become unscientific if not aligned with the winning shceme.

With this in mind, it is not surprising that the *vv* system was met with fierce political resistance. While the *vv* system admittedly has technical shortcomings, it has been demonized and criticized beyond what many consider reasonable, often for reasons that are based on misconceptions, supported by administrative decisions appearing to be made to taint the image of *vv* in the eyes of the public. In the following, we will describe the *vv* system, its shortcomings and the criticism it has drawn. We will also describe and briefly analyze alternatives that have been proposed by its critics.

2 Voter Verifiable DREs

As mentioned, the *vv* system is based on adding a printer to each DRE machine, allowing for the voter to inspect his vote before approving it and having it counted. The approved votes are entered into a sealed container (a plastic bag), allowing for later recounts.

What if the voter does not accept the printed vote? If a voter finds that he has entered the incorrect choices after seeing the printed paper slip, he may cancel the vote and start over again. Similarly, if a voter claims that the information on the screen diverges from the information on the slip (or either is different from the selection he made) then he can request that his vote be canceled and votes again. If the alleged mismatch persists, the entire precinct has to switch, from then on, to performing manual voting.

This way to deal with potential inconsistencies has, on one hand, been demanded by critics who later held it as an inherent inconsistency of electronic systems forced to turn voter-verifiable, while, on the other hand, exposed a peculiar double standard: before the *vv* measure, if the voter repeatedly complained of mismatch between the information keyed in and the information on the screen (whether this occurred or not), then he would have to accept whatever the screen says or give up his right to cast a vote. The justification was that since vote is secret, no one was allowed to verify his claim and/or suspend the use of the equipment upon such claim. Printer-screen inconsistencies are thus feared as a much wilder beast than keyboard-screen inconsistencies.

Do the printed slips favor vote selling? In a misinformed attempt to ban the use of the *vv* system, it was even argued in Congress that its use is dangerous in that it allows a voter to take the printed receipt of his vote to the candidate to whom he wishes to sell his vote [17, 18]. This is clearly not the case, since the voter never obtains the printed slip, but only gets to see it behind a window.

The irony here is that a simple way to sell votes remains, with or without the use of *vv*. Since the *DRE* voting software displays the name and a picture of the chosen candidate before the voter confirms his choice for that vote, and since this picture is from a file provided by the candidate to official authorities in charge of setting up the software, we have that a candidate could later show a voter a collection of different pictures of him or herself, one of which is identical to the one given to the electoral officials. This way, the candidate could pay voters able to pinpoint the correct picture. A savvy voter could, of course, select the candidate and then cancel his vote, thereby being able to recognize the picture without voting correspondingly – most voters, however, are not likely to do this.

Do the added printers cause difficulties? Before being banned, the *vv measure was the subject of a "compromise" [3]. Given the public outcry from the earlier senatorial scandal, the* vv *system was to be employed, "on a trial basis", in 3% of the precincts in the October 2002 election in which Brazilians voted for president, state governor, two Senate and two House seats [4]. Interestingly, media attention after the election was not focused on analysis of the results of the election, not even on some strange mishaps, such as a momentary drop in the partial total of votes officially tallied for a presidential candidate, from over one million to minus forty one thousand [5, 6]. Rather, it covered the long lines at polling places, which were worse in those with* vv *add-on printers. Nevertheless, the likely reasons for these additional delays were never mentioned [8].*

Among these reasons, we have that the election officials in charge of setting up the machines were not instructed to remove a "security" seal blocking the exit path of the slips of paper from the small add-on printer before sealing the bag onto it. As a result, the seal (which was explicitly specified at the printer supplier's contract) caused the printers to jam. Another reason is that voters were not told about the need to push the confirm key twice *to have his vote approved* and *have the slip cut from the reel and moved to the sealed bag. Failing to do so caused the voting machines to time out after two minutes, requiring them to be reset using a tortuous menu path, and requiring the precinct official to enter a password. A third reason is that the number of voters registered by the electoral administration to vote at most* vv*-enabled precincts were increased beyond historic top levels. As a result of the "bad experience" with the* vv *system, congress quickly voted, one year after this "trial", not to use it in future elections [10].*

Were the auditing features employed? *After the compromise allowing the "trial" of the* vv measure in 3% of precincts, and before the 2002 election running it, there were several warnings by high-ranking officials from the electoral administration of the risks posed by such a mechanism for vote paper audit. Its functionality – to provide voter verifiability – was deemed as an "unnecessary" and "stupid" security measure which could taint the success of an otherwise flawless election [9]. Given the very tight margins (less than 0.2%) of one state gubernatorial runoff election, one for which pre-vote polls yelded up to 8% discrepancy, the losing candidate, relying on the "trial", appealed for a manual recount of the votes of the *vv*-enabled precincts. His appeal was dismissed by the local electoral tribunal, headed by an early critic of the *vv* measure [9], on the grounds that a manual recount from a non-mandatory mechanism "could put under suspicion [the electronic] elections nationwide" [11]. After all, they would argue, no one has yet been able to prove there has been any fraud at electronic votings in Brazil. The main question remaining: is no one able to prove fraud because the system is secure, or is the system secure because no one can prove fraud? In other words, secure for whom and against what? For layman voters against fraud, or for dishonest insiders against recounts?

3 Alternatives

Three alternatives to the *vv* measure has been brought forward by its critics. We will briefly describe these, along with their relative weaknesses.

Alternative 1: Parallel voting. The first alternative is called *parallel voting*; under this proposal, a sample of the voting machines that are to be used are replaced by backups, and a test is run on that sample during election hours. The test consists of running a "simulated election", in which a group of electoral officials enter votes on the selected machines as if they were individual voters, to verify that they operate correctly. This is done by checking that the machine output is

correctly generated for the votes cast by the officials, at the end of the voting period. The final simulated tally is then compared to the expected tally, this one run by anyone following the test. Any discrepancy can be detected, since the choices for the simulated votes are drawn and publicly known.

The main weakness of this proposal is that the conditions set up for the simulation would differ significantly from the "real" conditions. Most notably, given the complexity of the routines for entering a simulated vote [13], this task is made much more time consuming than at the standard vote (as described in [15]). Therefore, if the *DRE* is controlled by a malicious piece of software, the test situation can then be detected and the *DRE*'s behavior affected. Note that although the time to key in the choices for a vote are indistinguishable, it is highly unlikely, in a real vote situation, that the votes be cast at the very low rate which is possible at simutation. Therefore, the software of the *DRE* can determine, from the number of votes entered by the end of the voting period, whether to run the correct tallying (if a test was detected) or to "cook the books" (if a real-election situation was detected) before it outputs.

Alternative 2: Software auditing. This naturally brings us to the second proposal, which is to have the software purported to run on the *DRE*s audited for correctness. Given the complexity of the software used and the difficulty of establishing *exactly* what a piece of software does (as evidenced by the continuous use of bloated commercial general purpose software), this is not likely to be a meaningful solution.

To make it worse, inspecting the system's code has proven to be a charade, with repeated promises – and rulings – to "open all the code" failing to materialize at the last moment, election after election [13, 14]. Even though auditing of the *complete* source code is required by law since 1997, only parts of such code has been offered for inspection. This is in spite of the most rigid non-disclosure agreement possible, allegedly due to "copyright protection issues". Moreover, even if this were not the case, practical circumstances come in the way of making this alternative a satisfactory solution. For one thing, there have been no way offered (or permitted) to verify that the audited code is the same as that which is used on election day, making such "code audit" a silly exercise. Besides the code of operating systems not been included, the time and conditions allotted for inspection has been very far from sufficient, making it clear that this alternative is unconvincing except as a public relations stunt.

Alternative 3: Cryptography. A third and latest proposal has been to use additional electronics and/or software to generate and verify digital signatures on various portions of source and executable code, so that interested parties can verify that these are the components which are later compiled and used. The resulting executable, along with further signatures and verification software, would then be deployed to the hardware constituting the 450,000 *DRE* machines typically used in an election. During or after the deployment process local supervisors could then verify their party's signature on appropriate files – using the verification software deployed within the *DRE* software [14].

However, if the verification software is tweaked before deployment so as to not report errors, nothing would be gained by running it. Furthermore, even if the deployed verification software is working properly, the *DRE*'s operating system could have been tweaked to defeat its intended objective, namely by presenting the original file to the verification software, to later replace it by a hidden and rigged version. That is to say, the operating system (which was left out of the inspection set up by measure two, as the reader may recall) can shelter code designed to override any of the security measures intended to be taken by this approach. In other words, if the short-circuited nature of this verification would not be enough to invalidate alternative three, the software to be verified has always

included binaries untraceable by the 'auditing' permitted by alternative two, yielding a cumulative process without any basis of trust on which to build.

At this point it is worth noticing the difficulty of tracing the origin of the money spent to develop and deploy such *DRE* system, let alone the possible strings that may come attached. Interested parties have not been able to either validate the workings of deployed *DRE* machines, nor have they been allowed to inspect contracts in due time. Some of these contracts have never been made public beyond their summary or first outsourcing link, despite deemed public. The electoral administration was constitutionally set out in a way as to be its own judge, and the vast majority of voters and officials seem satisfied not only with such concentration of power, but also with the belief that technology works as panacea for negative human traits.

What are the benefits of these alternatives? The vulnerabilities of the three alternatives have been pointed out repeatedly to officials by various security experts. This leaves us with the question of whether the political support for these alternatives – and the resistance to the more straightforward *vv* approach – is grounded in incompetence or malice. We shall not attempt to address this question here.

4 Conclusion

Is Brazil, after all, ahead of its time regarding voting technology? Maybe.

It is understandable that voter verifiability measures tend to increase both the complexity of the system and the risk of malicious interference by individuals and organizations with rights to supervise election procedures. If not to affect the results, at least to cast doubt on the result, something a sore loser may consider. This, however, should not be taken as reason to discard such measures from the outset. Rather, it shall be held as motivation to better research e-voting systems, given that verifiability is a technical price to pay for automation. Brazil's pioneer experience with e-voting evidences the flawed nature of simplistic reasoning, while giving plenty of indications that election security is a matter of balancing risks, conveniences and responsibilities.

News indicate that Paraguay, Argentina, Mexico, and other countries where corruption and election fraud are not just abstract concepts, may soon borrow or rent Brazil's system. In the United States, where the same company dominates the procurement and supply of *DREs, serious debate on the convenience and possible effects of legal measures enforcing voter verifiability in electronic systems is under way. We thus may soon see a number of countries facing the same questions that Brazil has been led to face over the last few years.*

References

[1] National newspaper special report: "Crise no Senado, Tempestade no Planalto" *O Estado de São Paulo, May 2001 http://www.estadao.com.br/ext/especiais/tempestade/tempestade.htm, accessed July 27, 2003.*

[2] The 2002 Law implementing voter-verifiable measure: "Lei 10.408/02" D.O.U. de 11.01.2002, http://www.brunazo.eng.br/voto-e/textos/lei10408.htm, *accessed July 27, 2003.*

[3] Interview with Brazil's chief electoral official: "Ilmar Franco entrevista Nelson Jobim" *O Globo, Rio de Janeiro, October 15, 2001 http://oglobo.globo.com/pais/1659118.htm*

[4] Note in National newspaper: "CCJ aprova impressão do voto eletrônico" *Folha de São Paulo, pp. A9, October 29, 2001.*

[5] *National syndicated newspaper column:* "Coluna Jânio de Freitas", *Folha de São Paulo, October 8, 2002, São Paulo, SP.*

[6] *National syndicated newspaper column:* "Coluna Carlos Chagas", *Tribuna da Imprensa, October 10, 2002, Rio de Janeiro, RJ.*

[7] *Laerte Braga:* "A agência errada, o golpe é aqui, no Brasil" *http://www.crestani.hpg.com.br/2002C/laerte-braga.htm, accessed June 19, 2004.*

[8] *Local newspaper main stories on elections:* "Confusão Eletrônica" *pp.21,* "No Limite da Paciência", *pp.22, Correio Braziliense, October 7, 2002, Brasília, DF*

[9] *Interview with chief electoral official in Federal District:* "Fabrício Azevedo entrevista Lécio Rezende da Silva: Garantimos a lisura das eleições" *Jornal da Comunidade, August 4, 2002, pp.4, Brasília, DF.*

[10] *The 2003 electoral law bill:* "Câmara dos Deputados do Brasil - Proposição PL-1503/03, do Senado Federal" *Brazil's House of Representatives, National Congress http://www.camara.gov.br/sileg/Prop_Detalhe.asp?id=124899, accessed July 27, 2003.*

[11] *Editorial page from mainstream newspaper:* "Magela Recorre ao TSE para recontagem dos votos" *O Estado de São Paulo, November 19, 2002, São Paulo, SP http://www.estado.estadao.com.br/editorias/20-02/11/19/pol025.html, accessed July 30, 2003.*

[12] *Official web simulation of Brazil's electronic voting: http://www1.tse.gov.br/eleicoes/urna_eletronica/simulacao_votacao/urna.html accessed June 19, 2004.*

[13] *Official web site for Brazil's voting regulations: http://www1.tse.gov.br/servicos/resolucaoEm-Destaque/pesquisa.jsp accessed June 19, 2004.*

[14] *Brazil's Electoral Administration web newsroom: http://www1.tse.gov.br/servicos/informativo/-index.jsp accessed June 19, 2004.*

[15] *Report tracking Law 10.740/03's approval:* "Lei do voto virtual às cegas" *Forum do voto seguro, http://www.brunazo.eng.br/voto-e/textos/PLazeredo.htm, accessed May 10, 2004. Links doc.1 through doc.10 in report point to scanned versions of paper documents showing: a) trail the corresponding bill would have followed in Congress; b) its logical inconsistency.*

[16] *Public manifesto:* "Alerta contra a insegurança do sistema eleitoral informatizado" *Forum do voto seguro, http://www.votoseguro.com/alertaprofessores, accessed May 10, 2004, with 878 signataries.*

[17] Transcripts of House evening session of October 1st, 2003*: Brazil's House of Representatives, National Congress http://www.camara.gov.br/Internet/plenario/notas/ordinari/v011003.pdf, accessed May 10, 2004, pp.333-334: speech by the leader of Workers Democratic Party (PDT), Rep. Alceu Colares, denouncing: a) false representations by Rep. Moroni Torgan about the 2001 vv measure, which the bill there and then under vote would ban; b) the rigging of the House's internal electronic tracking system, on the path taken by said bill.*

[18] *Excerpt from* official video transcripts of Brazil's House of Representatives evening session of October 1st, 2003*. Forum do voto seguro www.brunazo.eng.br/voto-e/arquivos/collares1.rm [codec Real video 3.0, aprox. 3 min, 4.5Mb]:*

Speech by PDT Leader (referenced in [17]), who frantically waves paper trail documents (scanned and linked in [12]) which show a rig at the House's internal electronic tracking system, on the path taken by the bill there and then under vote, to an unamused and unresponsive House president (Rep. João Paulo Cunha) conducting the session.

www.brunazo.eng.br/voto-e/arquivos/collares2.rm [codec Real video 3.0, aprox. 7 min, 8.5Mb]: Complete speech.

The author

Pedro Antonio Dourado de Rezende is a tenured professor at Computer Science Department, University of Brasilia (UnB). ATC PhD in Applied Mathematics from University of California at Berkeley in 1983, heads the UnB Cryptography and Info Security Extension Program since 1997. Author of over one hundred articles on related topics, is a member of Brazil's Public Key Infrastructure Steering Committee since 2003, by appointment of President Lula da Silva to represent civil society.

This article is based on an earlier copylefted version published at www.cic.unb.br/docentes/pedro/trabs/election.htm