Security and Threats in the Brazilian e-Voting System: A Documentary Case Study Based on Public Security Tests

JÉSSICA I. PEGORINI,
Federal University of Paraná State, Curitiba, Brazil, e-mail: jipegorini@inf.ufpr.br,
ALINNE C. C. SOUZA, ANDRÉ R. ORTONCELLI, RODRIGO T. PAGNO, and NEWTON C. WILL,
Federal University of Technology - Paraná, Dois Vizinhos, Brazil,
e-mails: {alinnesouza,ortoncelli,rodrigopagno,will}@utfpr.edu.br,

Democracy is one of the processes that has become electronic over the years, and Brazil, as one of the countries with the largest democracy in the world in terms of number of voters, has also started the informatization of the voting process. However, it is important to note that, in addition to advantages that an all-electronic voting process brings to an election, such as rapid vote tabulation and the availability of results, there are technical issues to be addressed to prevent fraud and system failures, ensuring a fair process. In this sense, this paper presents a case study that analyzes what are the problems faced in the Brazilian electronic process by studying public reports released by the authorities. Brazilian e-voting system has several security mechanisms, such as voter authentication by biometrics, and is capable of detecting unauthorized modifications. Our findings show that, despite the Brazilian e-voting technological evolution, the system still faces some problems that can compromise the outcome of an election, and also bring some doubts about the procedures defined for carrying out public security tests in the e-voting system.

CCS Concepts: • **Applied computing → Voting / election technologies**; *Law*; • **Security and privacy → Systems security**; *Symmetric cryptography and hash functions.*

Additional Key Words and Phrases: electronic voting, electoral system, information security, security tests, Brazilian elections

ACM Reference Format:
Jéssica I. Pegorini, Alinne C. C. Souza, André R. Ortoncelli, Rodrigo T. Pagno, and Newton C. Will. 2021. Security and Threats in the Brazilian e-Voting System: A Documentary Case Study Based on Public Security Tests. In *ICEGOV 2021: 14th International Conference on Theory and Practice of Electronic Governance, October 06–08, 2021, Athens, Greece.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Since an election is a means by which the population expresses its right to democracy, many countries have been evolving their voting process, adopting electronic voting systems. These systems can be placed in two categories: supervised and remote. In supervised e-voting the voter uses physical voting machines at specific locations, while in remote e-voting the vote can be registered by the Internet, using their own computer or smartphone [22].

Brazil uses a supervised e-voting system, with the voting machines maintained by the Superior Electoral Court (SEC)[1], which is responsible for the entire Brazilian electoral process. This system requires strong protection mechanisms, to ensure the security of the data and process itself. In order to an election to have credibility, it must be transparent, complete and authentic and, above all, the voter must be sure that his vote is totally anonymous.

Seeking to improve the system, Brazilian Electoral Justice[2] carry out internal tests and also promotes Public Security Tests (PST), where experts can carry out attack plans against the Brazilian Electoral System. The breaches found by the experts are reported, documented and then SEC is ensured to apply appropriated corrections [18].

This paper aims to compile and analyse all attack plans presented in five editions of PST, assessing the security of Brazilian Electoral System, and reporting what breaches the voting machines and the system is susceptible to. We also seek to explore the limitations of PST, since it does not cover all aspects of the electoral process.

[1]Maximum body of the Electoral Justice, which plays a fundamental role in the construction and exercise of Brazilian democracy.
[2]Specialized branch of the Judiciary that acts on issues related to Brazilian elections.

The remainder of this paper is organized as follows. Section 2 provides background information about the Brazilian e-voting system, with technological and legal information. Section 3 describes the public security tests, that are carried out by the SEC and allows researchers and professionals to test the electoral system and find vulnerabilities. Section 4 presents how this study was conducted, with the definitions and methods employed. Section 5 summarize the findings described in the PST reports, listing the vulnerabilities found and proposed solutions, while Section 6 discusses the good and ugly about the PST carried out so far. Section 7 presents previous research closely related to our paper. Finally, Section 8 concludes the paper.

2 BRAZILIAN E-VOTING SYSTEM

Brazil is one of the largest democracies in the world, where about 80% of the electoral population actively participates in elections [2]. Currently, the Brazilian Electoral System is totally electronic, but there was a time when the reality was totally different, with the voter speaking his vote to a clerk, who took notes and then making the vote tabulation. In the time of the Empire, and in the early years of the Republic, there was no official ballot, so voters deposited any paper bearing the candidate's name into ballot boxes. The choice could also be made only if the voter spoke the name of his candidate aloud [21].

Voting secrecy was guaranteed to voters in 1932 with the creation of the Electoral Justice, which brought the voting booths and official ballots for voting. Voting ballots started to be deposited at the ballot boxes by the voter, in envelopes manufactured by the Electoral Justice [21]. The Electoral Code, also from 1932, has provisions for the use of voting machines, and the search for the automation of the electoral system led to the construction of many projects of voting machines, but none of them was adopted [8].

The electoral system evolved over the years, and in 1989 an experimental computer was used for a computerized voting section in Brusque city. At the time, voters used the computer for the second round of presidential elections, and another computer, installed at the SEC, received the information. This was the starting point for the voting computerization process [25].

In 1994 occurred the first vote tabulation of a general election using a computerized system located at the SEC, and the electronic voting process started in the following year, when a committee of jurists and IT professionals presented a prototype of a voting machine. The new voting machines were introduced in the country in 1996, but only in 2000 the elections became entirely electronic [27].

2.1 Voting Machines

The development of the voting machines currently used in Brazil began in 1995, from a project created by the SEC and, despite having several versions, all voting machines are composed of an electoral terminal used to identify the voter, and another for identify the votes. These two devices are physically connected by a cable, and as soon as the voter is identified, their data appears on the terminal used to verify the voter, and the voter will be able to register their votes in the voting machine via keyboard [5].

The voting machine, called Direct Recoding Electronic (DRE), is a computer running a Linux based operating system, developed by the Brazilian Electoral Justice. The software runs in a dedicated chipset, in standalone mode, and software and data are stored in a memory card. The voting machines do not have any type of network hardware, which makes it impossible to connect to the internet, Bluetooth or other devices. They start operating at 8 a.m. on voting day, and from 5 p.m. they print the *poll tape* (or "*boletim de urna*"), and no more votes are accepted [6].

For each election, voting machines are loaded with a set of 28 applications developed by the SEC, mounting the "voting machine ecosystem", which is responsible for the automation of activities and processes for its proper operation [27]. The main applications in the voting machine ecosystem are:

- GEDAI-UE: Data Management System, Applications and Interface with the Voting Machine, which is responsible for the loader, voting and media flashes for the voting machine, in addition to receiving and sending correspondence to each Regional Electoral Court (REC);
- SCUE: Voting Machine Loading System, installs the operating system, election data and generates a unique number for each voting machine;
- ATUE: Voting Machine Self Test System, which is responsible for performing a self test to check the voting machine components in order to verify that they are working properly;
- VOTA: Collects and counts the votes of an electoral section.

In addition to the voting machine ecosystem, they also have a set of 90 systems for voting machines, which are sealed and sent to the REC, so that they can proceed with the individual installation in each voting machine. Each voting machine also receives information about candidates and memory cards that store a copy of the votes on election day.

SEC also uses the Installation and Security System (ISS), a set of applications and drivers for the Windows operating system, which creates a security infrastructure and ensure access control for Electoral Justice applications. ISS monitors and protects all computers integrated into the electoral process in the country. ISS also monitors the entire life cycle of the election, from voter and candidate records to the generation of databases for electronic voting machines, reception, transmission and dissemination of results [27].

All systems used by the voting machine are sealed and digitally signed at the Digital Signature and Systems Sealing Ceremony, a public event required by law that takes place in the SEC, with the participation of political parties, coalitions, Public Ministry, Brazilian Lawyer Association and authorized people. On that occasion, the hash of the sealed programs is generated, so that the authenticity of the voting machine can be proven at any time. Electronic voting machines also have practices and devices to ensure that it is not physically violated [21].

2.2 Zero Tape and Poll Tape

Zero tape (or "*zerésima*") is a report generated right after the initialization of each voting machine, and shows that it has no stored vote. This document is signed by the president and the secretary of the polling station, and also by party inspectors who are present at the polling station [27].

At the end of the election, five copies of the *poll tape* (or "*Boletim de Urna*") are printed, which is the report containing all information from the polling station, with the number of votes to each candidate. The poll tape is also signed by the president and secretary of the polling station and also by party inspectors. Also, the generated file is encrypted, digitally signed and then transmitted to the *Transporter* by removing the voting machine memory card. Transporter is responsible for validating the compatibility of the poll tape's digital signature public key with its private key and decrypting it for data recovery. The voting machine memory if physically transported to the Transporter machine in a package sealed that is also signed by the president of the polling station. [26].

The *Digital Record of the Vote* (DRV) is the file responsible for registering all votes, recording what was typed in the voting machine, and it is from the data in this file that the zero tape and the poll tape are generated. Since it does not register any additional information, it is hard to link the vote with a respective voter, as each vote is stored in a random position in the file. This file is very important tool for auditing the tabulation of a pooling station [27].

2.3 Transmission of Results and Tabulation

Elections end at 5 p.m. in each of the polling stations, when the president of the polling station generates the poll tape, using his own password. Five copies are printed: three are sent to the Electoral Registry; one is fixed outside the polling place; and the last one is delivered to the party representatives. The data stored in the voting machines are digitally signed and recorded on the results media, which is encrypted using standards algorithms defined by

the SEC. These data are sent to the transmission centers through an encrypted network, used exclusively by the Electoral Justice [27].

Electoral Courts have security mechanisms developed by the Electoral Justice, to ensure that the information that leaves the voting machine reaches its destination without any change. The transmission channel used to send the data also receives an encryption layer, preventing external attacks. REC also perform data verification to check the data integrity, by decrypting the files and checking the digital signature, to prove that the data received comes from the voting machines of the Electoral Justice.

The files are verified via digital signature and the poll tape are decrypted by using the key of the tabulation system, which makes the poll tape readable. After check the data, they are forwarded to tabulation and publishing, and the null and white votes are not considered in the sum of the valid votes. The results are forwarded to the SEC in Brasilia, which is responsible for tabulation and publishing, which can be monitored in real time, and it is possible to follow the evolution of the tabulation every minute [27]. All steps performed after closing the polling station are shown in Figure 1.

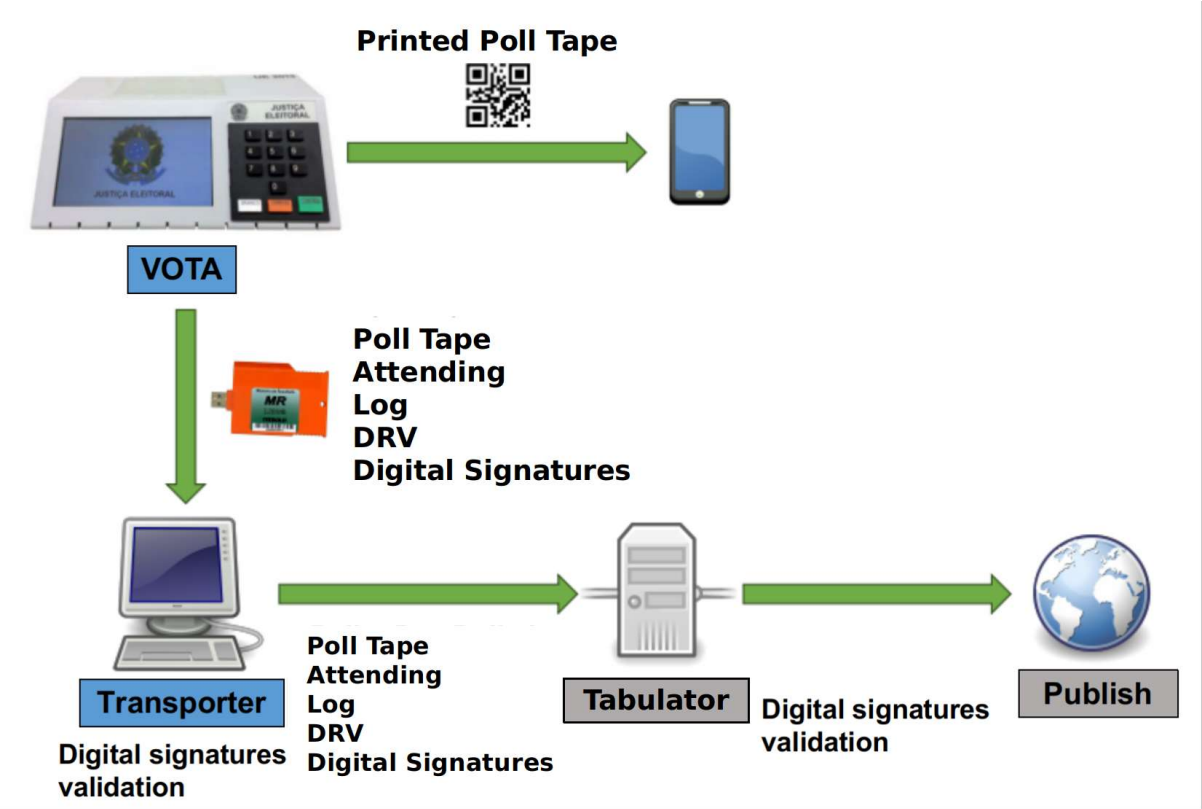

Fig. 1. Transmission, tabulation and publishing voting results.

3 PUBLIC SECURITY TESTS

Public Security Tests (PST) are events promoted by the Brazilian Electoral Justice that gathers several experts in computer science, in order to carry out attack plans against the security mechanisms of the Brazilian Electoral

System, in an attempt exploiting known or unknown vulnerabilities. These events allow to reveal eventual threats and vulnerabilities, in the procedures and in the process itself. In addition, the event also aims to test the trustworthy of the polling and vote tabulation, checking the system robustness and maturity, in order to make constant improvements in the whole process [18].

PST is carried out following three stages that involve the preparation, execution and evaluation of the event. Each expert (or group of experts) must register their attack plans, which will be revised and validated by SEC. Accepted attack plans are executed by the experts and then the evaluation committee analyzes the test reports of each expert, and produces the final report that presents the results achieved. The event also has support commissions with SEC members, who guarantee the execution of the event as scheduled [18].

The first edition of PST was held in 2009, where researchers from different institutions and areas of information technology carried out different attack plans against the system and the exposed ideas contributed to the technological improvement of the voting process. The following edition of the event occurred in 2012, and the researchers were able to participate in the preparation phase of the voting machines, having access to its source code and they could learn more about the peculiarities of the system and carry out their attack plans [18].

Despite the success of the event, SEC received some criticisms and suggestions regarding the methodology used in the evaluation of the work developed by the researchers, and chose not to realize the event in 2014, so that it could review the evaluation methodology, in order to improve the event for the following editions. The following event occurred in 2016, with several researchers achieving the expected results. The same occurred in the year 2017, when investigators detected some bugs in the system, being able to explore some vulnerabilities. The most recent edition of PST was held in 2019, and achieved positive results for one group of researchers, which using a light version of the system and reverse engineering techniques, were able to succeed in executing the test plan [18].

4 RESEARCH METHOD

This section describes how the case study was conducted, from its planning, data collection and analysis.

4.1 Case Study Design

The main objective of this study is to investigate the occurrence of failures and vulnerabilities in the Brazilian Voting System, by security technicians and experts, during the PST editions carried out by the Electoral Justice. For this, a comparison of the results of the five PST editions was performed aims to verify if the failures and vulnerabilities were fixed or reoccurred in the next edition. Furthermore, it was also analyzed whether these problems were fixed before the election took place.

In order to address this objective, we observed the methods to identify failures and vulnerabilities; countermeasures to address failures and vulnerabilities identified; and successful and unsuccessful attack plans. Thus, we defined two research questions:

- **RQ1: Which failures and/or vulnerabilities were identified in the PST?**
  Rationale: This question seeks to answer if failures and vulnerabilities were found during the PST editions, and what were those failures and vulnerabilities. As a result, the answer for this question can serve as to make improvements and refinements in the electoral system.
- **RQ2: How failures/vulnerabilities identified in the PST editions were fixed?**
  Rationale: Identifying how solutions fixed the failures and vulnerabilities reported by the IT experts. We would like to develop an understanding of how these solutions can aid to obtained constant improvements in the whole process of the electoral system.
- **RQ3: Is the PST adequate to assess the security of the Brazilian voting system?**
  Rationale: We seek to assess whether the PST is effective as a mechanism to test the security of the voting

machines and the voting system. The answer to this question can lead to recommendations to improve the security tests performed on the voting system.

4.2 Data Collection Procedures

There are several different sources of information that can be used in a case study. The main source of information in this investigation is the archived data. With this source, an independent analysis is performed where already available and sometimes compiled data is used [28].

In this method, the failures and vulnerabilities, countermeasures to address failures and vulnerabilities, and successful and unsuccessful attack plans variables could be captured. The archives data used in this study consists technical reports that contain information about each of the PST editions, which are published on the Electoral Justice website [18]. These reports are written by a technical commission and includes all the attack plans carried out in the electoral system, as well as the results obtained.

The data was collected and analyzed simultaneously, in incremental and iterative steps to answer the research questions.

4.3 Analysis of Collected Data

The analysis aims to derive conclusions from the data, keeping a clear chain of evidence. The chain of evidence means that a reader should be able to follow the derivation of results and conclusions from the collected data [29].

This study analyzed the collected data qualitatively through grounded theory. This technique was used to code, categorize and synthesize the data of each PST edition, as proposed in the constant comparison method [7]. The coding process involves attaching codes, or labels, to pieces of text that are relevant to a particular theme or idea of interest in the study. After coding the transcriptions, the codes were reviewed to identify similarities, duplicates, or misleading codes. The codes discovered from the transcription of each PST edition were constantly compared to codes in the same edition and from other PST editions. A code list was categorized considering the interest of the research questions, which contains: *(i)* failures and vulnerabilities; *(ii)* countermeasures; *(iii)* successful attack plans; and *(iv)* unsuccessful attack plans.

5 FINDINGS

This section examines the results achieved regarding the data collected in the public reports made available by the Electoral Justice. The results of our case study are shown according to the PST editions.

5.1 First PST Edition (2009)

The year of 2009 set the beginning of PST, which occurred between November 10 and 13. We observed that the voting system presented no major vulnerabilities in the tests performed, where no investigator was able to alter the destination of the votes or break the secrecy of the vote. Some attacks allowed changes or insertion of files, but they had no major consequences due to the defense mechanisms of the voting machine. SEC points out that some of the security control mechanisms of the real operating system have been disabled to carry out the PST, in order to make it easier for investigators to carry out their attack plans.

One of the investigators aimed to break the secrecy of the vote by capturing the electromagnetic radiation emitted by the keyboard of the voting machine during the voting. These radiations allow you to monitor the typing of numbers on the voting machine keyboard, which could lead to the identification of the vote. The test was partially successful, since the distance between the radio device and the voting machine was only five centimeters and, taking into account that in a real scenario the voting machines are in an isolated environment and under surveillance in the polling stations, this is not viable type of attack. Despite this, the voting machines manufactured later started to encrypt the terminal keys, so that a different electrical signal is produced each time a key is pressed, preventing any attempt to identify a pattern of key pressing. Other investigators tried to

insert a file into the voting media, but this action was rejected by the voting machine system. Also, two other changes to system files were immediately detected by the voting machines' security modules. The change of a file, the attempt to generate the media without the use of the media generator, and the attempt to start the system through another program were prevented by the security barriers of the electronic system, mainly by digital signatures and the use of encryption mechanisms [12].

5.2 Second PST Edition (2012)

The second edition of the PST occurred three years later, between March 20 and 22, 2012. Among the large number of attack plans sent, many did not present any important contribution to improve the process of the system, and some of them were not properly concluded, thus not being evaluated by the commission. One of the groups was successful in executing the attack plan due to an error in the *Digital Record of the Vote* (DRV), where the written sequence is deterministic and can be derived independently from the public products of an election. Upon having possession of the DRV, it was possible to redo the sequencing of votes, but SEC says that is not possible to violate voter secrecy, since the group was unable to obtain the sequence of voter attending, and thus it was impossible to relate the votes in the file with the voters [13]. Despite this, it was demonstrated that the vote can be linked to the voter even if the data is randomized [4].

According to SEC, the results achieved by this test was a valuable contribution to the improvement of the process, but points out that there is no way to relate a vote to one person, since in the testing phase the team had access to all source codes used in the voting machine, which does not happen in a real election. He also commented that the test managed to write the order in which the votes were entered in the voting machine, but it would be unlikely to be able to relate to voters, because the voting occurs on a first-come, first-served basis, and the list of voters is available in the polling station is in alphabetical order [13].

5.3 Third PST Edition (2016)

This PST edition was realized in 2016, on March 8, 9 and 10. We observed that there were many successful attack plans. However, taking into account a real scenario, these results are unlikely to be a threat to the system, since it is necessary a breach in the electoral procedures, in addition to the corruption of the members involved. On the other hand, some tests were successful and made important contributions to the improvement of the system.

One of the investigators was able to access the poll tape and change its results, using it as an entry to the Ballot System (SA) of the voting machine and producing a new valid poll tape with fake results. In response, SEC corrected this problem by modifying the poll tape's verification code algorithm, now using an authenticator. To add a new layer of security, a QRCode with digital signature was also included in the poll tape, which allows interested parties to check its authenticity and integrity.

In addition to this vulnerability, another group of investigators also succeeded in executing their attack plan, being able to record the voting machine's audio instructions, which are used by blind people in voting. These instructions include the keys pressed and the vote confirmation. In the attack, audio was activated for each previously registered voter or for all voters in a previously configured section, without exceptions. The solution presented by the SEC was to restrict the use of audio only to previously registered voters or unlock it by the polling station president. In addition, whenever the audio is activated, a message is displayed on the voter's terminal alerting about the activation of this feature, and if the audio was improperly activated, the voter can ask the polling station official to suspend their vote and verify the equipment in the voting booth [14].

5.4 Fourth PST Edition (2017)

The fourth PST was held from 27 to 30 November 2017 and had 14 participants, divided into 4 groups and 4 individual participants. Several attack plans were rejected by the event's evaluation committee, and were not

carried out. On the other hand, some attack plans have been carried out, but have made no relevant contribution to improving the system.

In contrast, several tests were carried out successfully, presenting several contributions, among them, the leakage of the cryptography key from the voting machine media in the source code inspection environment, a bug in the digital signature check mechanism and absence of complementary digital signature in two system libraries. In this sense, SEC worked to correct these vulnerabilities, which the bug in the signature mechanism was corrected and the number of libraries was reduced. Software testing processes have also been improved by including a validated signature on all runnables, encryption keys present in the boot loader and the kernel have been removed and a key derivation mechanism was implemented based on information present only in the BIOS of the voting machine. Another point observed was the ability to boot the voting machine operating system in a virtual environment, aiming at carrying out possible reverse engineering in order to obtain cryptographic keys. In response, SEC enforced the encryption of the operating system in a way that only the voting machine is able to decrypt and start the system [15, 16].

5.5 Fifth PST Edition (2019)

The last edition of the event occurred between 27 and 30 November 2019. It is important highlight that 7 of 10 attack plans made no relevant contribution to improving the system, and one of them was not executed. Among the executed attack plans that made contributions, one group of the researchers were able to obtain a disk encryption key from the Installation and Security System (ISS) using reverse engineering techniques. The same group also carried out another attack plan with contributions, being able to alter data printed in the zero tape and in the poll tape.

The secrecy of the vote has not been compromised, and the integrity of the code has still been maintained. There was also a separate contribution, where an investigator suggested eliminating the standard “end of voting” sound during the preparation of the voting machine in the polling station, since voters who are already waiting in line can repeatedly relate the sound to some type of vote manipulation.

SEC listed the countermeasures to be implemented in the system to mitigate the detected vulnerabilities, which include the removal of the keys contained in the ISS source code. Another countermeasure adopted is the reduction of datasets registered in files by GEDAI-UE, use of previously signed data whenever possible and signature in the GEDAI-UE SQLite database. The poll start-up beeps will also be replaced by another audible signal to avoid confusing voters [17, 19].

6 DISCUSSION

In this section we discuss our findings from the reports published in the five editions of the PST and seek to answer the three research questions defined in Section 4.

6.1 RQ1: Which failures and/or vulnerabilities were identified in the PST?

A set of vulnerabilities and failures were found in the Brazilian electronic voting system in the five editions of PST. The first edition demonstrated the possibility of intercepting the numbers typed in the voting machine, breaking the secrecy of the vote. In addition, it was questioned the lack of standardization of procedures in Regional Electoral Courts in relation to the process of preparing the voting machines. In the second edition, the possibility of obtaining the voting sequence in a voting machine was demonstrated, even after the DRV had been randomized, and documented by [4]. Several possibilities of manipulating the kernel parameters for boot were also observed, opening backdoors for other attacks.

In the 2016 PST, it was demonstrated the possibility of replacing the voting machine flash card after the end of the elections, changing the votes before their transmission to the REC. The voting machines’s audio feedback feature, available to blind people, was also inadvertently enabled and made it possible to improperly record the

registered votes. In the fourth edition of the PST, the experts were able to obtain the cryptographic key (that was hard coded) of the memory card that performs the system loading to the voting machine, allowing the inspection of critical parts of the software and the leakage of other sensitive cryptographic keys. Also, it was demonstrated the execution of arbitrary code in the voting machine, allowing the insertion of anomalous texts at system startup, with the results reported in [2].

Finally, in the last edition of PST, experts demonstrated that it is possible to tamper with voting machine preparation data, which can bring damaging results to the election result. In addition, cryptographic barriers were broken down and experts had full access to the ISS and GEDAI-UE, which is used to generate the voting machines media.

6.2 RQ2: How failures/vulnerabilities identified in the PST editions were fixed?

After each PST edition, SEC releases a report describing what procedures will be taken to mitigate the problems found by the experts. To prevent the numbers typed from being captured by electromagnetic readings, the new voting machines are now equipped with an isolated keyboard, containing a dedicated ARM processor that encrypts the data before being sent to the voting machine system. SEC also applied some improvements in the Digital Record of the Vote (DRV), in order to ensure the anonymity of the vote. A set of encryption keys were removed from source code, the number of libraries used in the system was reduced, and other improvements were implemented in the encryption procedures. In addition, minor changes were applied to provide better feedback to the voter.

All these improvements were described in the PST reports, but it is difficult to describe how they were implemented, or even to ensure that they were implemented, since the source code of the systems used in the voting machines is not publicly available. Nowadays, the source code is available only to technical representatives of political parties, the Public Ministry, the Brazilian Bar Association and the Federal Police, among other entities. Making the source code public available would allow researchers and independent experts to analyze the system in a more complete and detailed way and would contribute to the transparency of the electoral process.

6.3 RQ3: Is the PST adequate to assess the security of the Brazilian voting system?

It is well known that the PST is a way for the Superior Electoral Court (SEC) to allow the evaluation of the hardware and software resources used in the elections by external members, but it is still far from covering all the aspects necessary for IT experts to be able to carry out a broad and detailed analysis of the process. SEC imposes several limitations to the participants of PST, as described by [24], including a short period of time to analyse all the source code from the voting machine systems, without the possibility to take notes or make changes in the code to understand how it works. In addition, there is no guarantee that the code examined in the tests will in fact be used in the elections, since the development of the system continues until the next election and may introduce new vulnerabilities.

Also, not all systems used during the election are subject to analysis by the experts. Despite the fact that, over the years, new systems are included in the hall of possibilities for investigation during the PST, important systems, such as the biometric identification, tabulation system, compilation environment, generation of cryptographic keys, post-election archives processing and voting machine preparation system are still out of scope.

Another issue is the fact that researchers must register their attack plans before the event, which will be analyzed by the SEC committee and can be rejected if they do not meet the requirements imposed. Such restrictions can bias the test result, since, knowing in advance the details of the attacks that will be carried out, SEC can add barriers that make it difficult to execute and give the impression that the system is secure. Despite this, the results obtained in the PST offer sufficient parameters to increase the system's resistance against external attackers, but the system may still present vulnerabilities against an internal attacker with privileged access. Finally, a set of recommendations for improving the scope of the PST are given by [4], [3] and [24].

7 RELATED WORK

Freitas et al. [10] aims to describe issues of evolution, challenges, logistics and security information based on the testimony of those responsible for the implementation and development of the Brazilian Electronic Voting machines. The results achieved by the authors highlight challenges overcome by the Brazilian Electoral Justice in the adoption of e-voting in the country. Perhaps the biggest one is the training of voters in the use and transparency of the system. Concerns about audits, costs and security are the main objections against electronic voting. When it comes to transparency, the system shows weakness, but official SEC representatives say that since 1996, when the voting machines were introduced in the country, there was no evidence of a proven fraud situation.

An approach seeks to analyze the question of the trustworthy of the Brazilian Voting System, analyzing the impact of this reliability on the 2014 presidential elections, considering the perception of voters' confidence in the system used by the country. Through a case study, the suspicion of fraud in the 2014 elections is emphasized, since the victory of a party that had already taken power 12 years ago was not fully accepted by the population. On that occasion, the opposition party requested to audit the results. The analysis carried out in the case study aims to investigate the reliability of the results of 2014, where the author concludes that, based on the information analyzed, the system appears to be safe and reliable, but there are factors that negatively affect the 2014 electoral structure. One of these factors is that the PST was not realized in the year prior to the 2014 elections. The author's final conclusion points out that no type of system is perfectly safe, electronic or not, and that the distrust factors found in the 2014 vote also would appear if the election was on paper. On the other hand, the credibility factors presented in the literature review conducted by the author are fulfilled, which may have been sufficient to guarantee the conduct of the election [1].

Aranha et al. [4] reports a vulnerability in the DRV that allows a complete violation of ballot anonymity, in addition to others flaws in the voting machine software and its development process. The authors discuss that the voting machines had no significant improvement in security in the period from 2002 to 2012 and that the Brazilian voting system does not satisfy minimal security and transparency requirements. Also, a paper report the experiences and discoveries during the PST occurred in the year 2017, where the authors, using specific tools and software, were able to identify potential vulnerabilities, where the most important was a vulnerability related to file system encryption [3]. The authors conclude that the voting machine used in the Brazilian elections still does not fully satisfy the minimum requirements of security and transparency. In addition, they made recommendations for the process, in order to provide stronger guarantees of their correct functioning on election day.

Another experience report is presented by [24], also from PST 2017. The author describes that the methodology adopted by the SEC for PST 2017 was not clear, and that the inspection in millions of lines of code of the programs used in the voting system should be carried out in just 3 days. A set of software and hardware used in the elections are not tested by the researchers in PST, such as the biometric validator and the software used to generate the cryptographic keys and to prepare the voting machines. The author also point out that there are the human factor in the security chain of e-voting system, since the voting machines are manipulated by several people in logistic process.

Finally, the transparency, security and organization of the Brazilian electronic voting system is discussed by [6]. The authors point out that the Brazilian voting machine is a black box and a postelection audit is almost impossible. In [20], the authors point out that the use of keys stored in source code, keys loaded into memory, unique keys and vulnerable or unverified cryptographic primitives indicate a lack of concern and commitment to security, in addition to the fact that there are no methods feasible to audit the results of an election. Also, [23] says that Brazilian e-voting system is a risky to democracy due to the lack of emphasis on security and the market-driven approach.

8 CONCLUSION

The history of e-voting in Brazil started in 1989, and in 1994 occurred the first vote tabulation using a computerized system. Only in 2009 the Superior Electoral Court (SEC) organized the first Public Security Test (PST), allowing IT experts to check the security of voting machines, and only in the next edition of PST, in 2012, the experts could share their findings and start a debate around the topic.

PST is an important initiative for the improvement of the Brazilian Electronic Voting System, aiming to test the security, integrity and authenticity of the system used in order to reveal vulnerabilities in it, given the opportunity to correct these vulnerabilities before the general elections. In addition, the event also aims to assess the trustworthy of the process and the security of confidential voting. Despite this, the PST does not cover all aspects and systems used in an election, and imposes a series of restrictions on participants, limiting the scope of the vulnerabilities that can be found.

Finally, there are still many concerns about the transparency of the voting machine and all the systems that make up the voting and tabulation processes, as described by [6]. Despite the fact that the process of votes transmission and tabulation is auditable through the poll tape, there are several discussions about the creation of independent mechanisms to audit the operation of the voting machines, including a paper trail to verify the votes stored in the voting machine memory [9, 11].

REFERENCES

[1] Luiz Fernando Abel. 2018. Trust in ICT for the Public Sector: e-Voting in Brazil's 2014 Election. *Planning and Public Policies* 1, 50 (2018), 379–398. https://www.ipea.gov.br/ppp/index.php/PPP/article/view/777

[2] Diego F. Aranha, Pedro Barbosa, Thiago N. C. Cardoso, Caio Luders, and Paulo Matias. 2018. Execution of arbitrary code in the Brazilian voting machine (in Portuguese). In *Proceedings of the XVIII Brazilian Symposium on Information and Computer Systems Security*. SBC, Natal, RN, Brazil, 57–70. https://sol.sbc.org.br/index.php/sbseg/article/view/4243

[3] Diego F. Aranha, Pedro Y.S. Barbosa, Thiago N.C. Cardoso, Caio Lüders Araújo, and Paulo Matias. 2019. The Return of Software Vulnerabilities in the Brazilian Voting Machine. *Computers & Security* 86 (2019), 335–349. https://doi.org/10.1016/j.cose.2019.06.009

[4] Diego F. Aranha, Marcelo M. Karam, André de Miranda, and Felipe B. Scarel. 2014. Software Vulnerabilities in the Brazilian Voting Machine. In *Design, Development, and Use of Secure Electronic Voting Systems*. IGI Global, Hershey, PA, USA, 149–175. https://doi.org/10.4018/978-1-4666-5820-2.ch008

[5] Diego F. Aranha, Helder Ribeiro, and André Luis Ogando Paraense. 2016. Crowdsourced integrity verification of election results: An experience from Brazilian elections. *Annals of Telecommunications* 71 (2016), 287–297. https://doi.org/10.1007/s12243-016-0511-1

[6] Diego F. Aranha and Jeroen van de Graaf. 2018. The Good, the Bad, and the Ugly: Two Decades of E-Voting in Brazil. *IEEE Security & Privacy* 16, 6 (2018), 22–30. https://doi.org/10.1109/MSEC.2018.2875318

[7] Pearl Brereton, Barbara A.Kitchenham, David Budgen, Mark Turner, and Mohamed Khalil. 2007. Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software* 80, 4 (2007), 571–583. https://doi.org/10.1016/j.jss.2006.07.009

[8] João Crisóstomo da Rocha Cabral. 1934. *Electoral code of the Republic of the United States of Brazil (in Portuguese)* (3 ed.). Freitas Bastos, Rio de Janeiro, RJ, Brazil.

[9] Rodrigo Carneiro Munhoz Coimbra, José Roberto Menezes Monteiro, and Gladiston da Silva Costa. 2017. Printed Record of the Vote, Authenticated and Guaranteed Anonymity (in Portuguese). In *Proceedings of the III Workshop on Electoral Technology*. SBC, Brasilia, DF, Brazil, 666–676.

[10] Jorge Lheureux de Freitas and Marie Anne Macadar. 2017. The Brazilian Electronic Voting System: Evolution and Challenges. In *Proceedings of the 2nd International Joint Conference on Electronic Voting*. TUT Press, Bregenz, Austria, 59–71.

[11] Fernando Teodoro de Lima, Mario A. Gazziro, Antonio de Abreu Batista Jr, Paulo Matias, and Joao V. C. Costa. 2017. Third Generation Electronic Voting Machine: A Prototype for Auditable Elections (in Portuguese). In *Proceedings of the III Workshop on Electoral Technology*. SBC, Brasilia, DF, Brazil, 677–685.

[12] Electoral Justice. 2009. Final Report of the Evaluation Committee of Public Security Tests in the Electronic Voting System (in Portuguese). http://www.justicaeleitoral.jus.br/arquivos/tse-relatorio-final-da-comissao-avaliadora-1o-teste-de-seguranca

[13] Electoral Justice. 2012. Security Test Reviews (in Portuguese). http://www.justicaeleitoral.jus.br/arquivos/tse-avaliacoes-sobre-o-teste-de-seguranca-da-urna-eletronica

[14] Electoral Justice. 2016. Public Security Test 2016 of the Public Voting System: Compendium (in Portuguese). http://www.justicaeleitoral.jus.br/arquivos/tse-testes-publicos-de-seguranca-2016-compendio

[15] Electoral Justice. 2017. Answers to vulnerabilities and suggestions for improvements found in the 2017 Public Security Test: Technical Report (in Portuguese). http://www.justicaeleitoral.jus.br/arquivos/relatorio-tecnico-tps-2017-1527192798117
[16] Electoral Justice. 2017. Report of the Evaluation Committee of the Public Security Test 2017 (in Portuguese). http://www.justicaeleitoral.jus.br/arquivos/tse-testes-publicos-de-seguranca-2017-relatorio-da-comissao-avaliadora
[17] Electoral Justice. 2019. Final Report of the Evaluation Committee (in Portuguese). http://www.justicaeleitoral.jus.br/tps/arquivos/tps_2019_relatorio_final-atualizado_17_12_2019.pdf
[18] Electoral Justice. 2019. Public Security Test (in Portuguese). http://www.justicaeleitoral.jus.br/tps/
[19] Electoral Justice. 2019. Vulnerabilities and Suggestions for Improvements Found in the 2019 Public Security Test: Technical Report (in Portuguese). http://www.justicaeleitoral.jus.br/tps/arquivos/tps_2019_relatorio_tecnico_atualizado_17_12_2019.pdf
[20] Isadora Garcia Ferrão, João Otávio Chervinski, Sherlon Almeida Da Silva, Diego Kreutz, Roger Immich, Fábio Kepler, and Rodrigo Da Rosa Righi. 2019. Electronic voting machines in Brazil: timeline, evolution and failures and security challenges (in Portuguese). *Brazilian Journal of Applied Computing* 11, 2 (2019), 1–12. https://doi.org/10.5335/rbca.v11i2.9056
[21] Luciano Felicio Fuck, Mauricio Caldas de Melo, Janeth Aparecida Dias de Melo, and Renata Leite Motta Medeiros. 2016. Electronic ballot box, 20 years in favor of democracy (in Portuguese). https://bibliotecadigital.tse.jus.br/xmlui/handle/bdtse/6439
[22] Robert Krimmer, Melanie Volkamer, and David Duenas-Cid. 2019. E-Voting – An Overview of the Development in the Past 15 Years and Current Discussions. In *Proceedings of the 4th International Joint Conference on Electronic Voting*. Springer, Bregenz, Austria, 1–13. https://doi.org/10.1007/978-3-030-30625-0_1
[23] José Rodrigues-Filho, Cynthia J. Alexander, and Luciano C. Batista. 2006. E-Voting in Brazil - The Risks to Democracy. In *Proceedings of the 2nd International Conference on Electronic Voting*. Köllen Druck, Bregenz, Austria, 85–94.
[24] Rodrigo Cardoso Silva. 2020. The Public Security Test of Brazilian E-Voting System: The Challenges in Pre-Electoral Observation. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*. ACM, Athens, Greece, 349–358. https://doi.org/10.1145/3428502.3428550
[25] Carlos Macedo Silveira. 2011. From paper to electronic voting: A case study of the implementation of biometric voting in Canoas/RS (in Portuguese). *Journal of Strategic Studies* 34, 2 (2011), 281–293. https://doi.org/10.1080/01402390.2011.569130
[26] Superior Electoral Court. 2019. Ballot Box Security: Cryptography (in Portuguese). http://www.tse.jus.br/eleicoes/urna-eletronica/seguranca-da-urna/criptografia
[27] Superior Electoral Court. 2021. The History of Electronic Voting. https://english.tse.jus.br/news/the-history-of-voting
[28] Claes Wohlin, Per Runeson, Martin Hst, Magnus C. Ohlsson, Bjrn Regnell, and Anders Wessln. 2012. *Experimentation in Software Engineering*. Springer, Berlin, Germany. https://doi.org/10.1007/978-3-642-29044-2
[29] Robert K. Yin. 2013. *Case Study Research: Design and Methods* (5 ed.). SAGE Publications, Nova York, NY, USA.