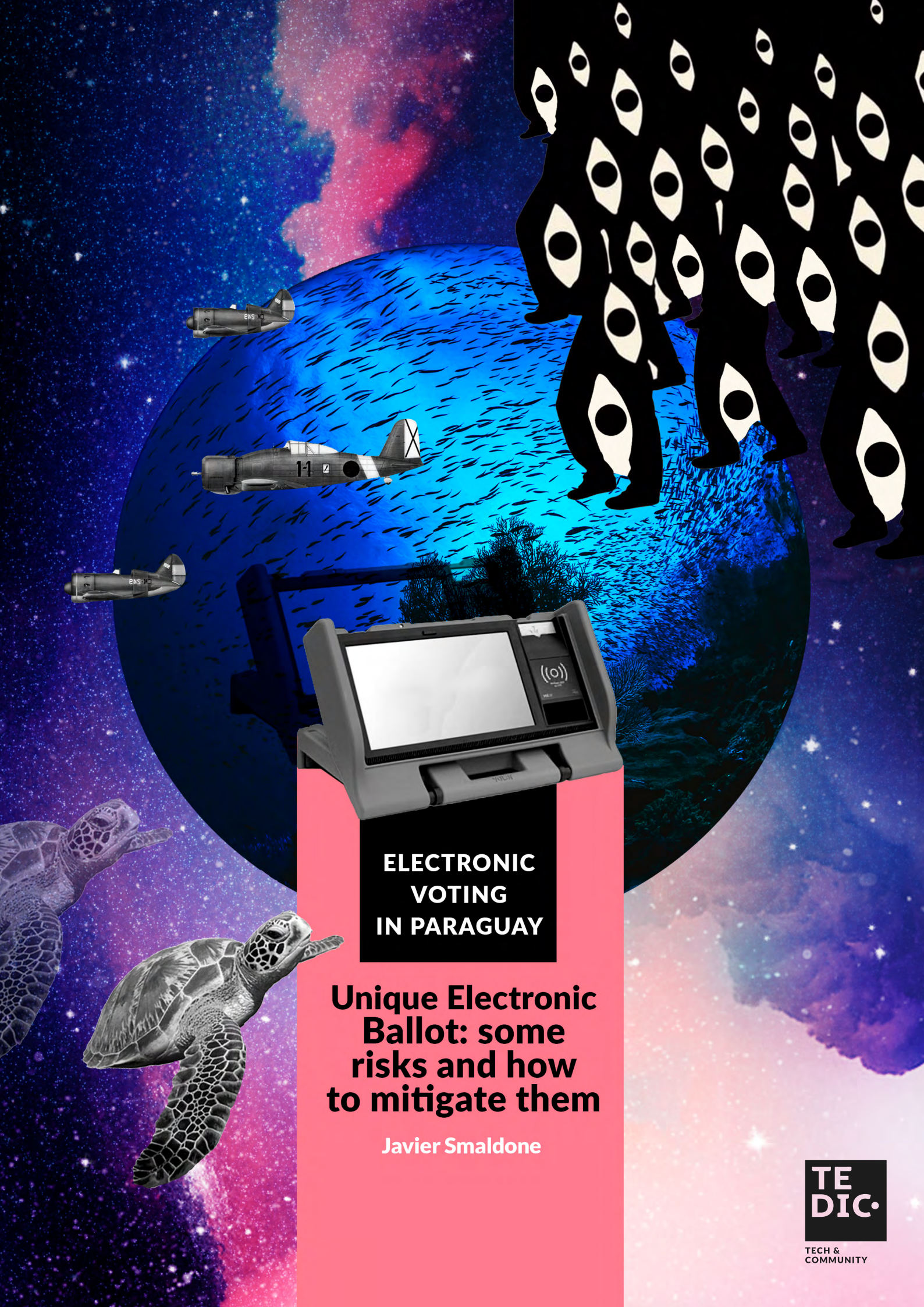


ELECTRONIC VOTING IN PARAGUAY

Unique Electronic Ballot: some risks and how to mitigate them

Javier Smaldone

TE DIC·
TECH & COMMUNITY

Unique electronic ballot: some risks and how to mitigate them

Javier Smaldone

This white paper was written as part of the TEDIC endeavor within the framework of a project funded by the National Endowment for Democracy (NED).

This white papers series seeks to guide and inform in a concise and extensive way about electronic voting from a political, legal, philosophical, technical, social and cultural perspective. It is intended to help you understand this complex subject in depth.

TEDIC
TECH & COMMUNITY

TEDIC is a non-governmental organization founded in 2012, whose mission is to defend and promote human rights in digital environments. Among their main topics of interest are freedom of expression, privacy, access to knowledge and gender on the Internet.

Coordinatin: Maricarmen Sequera

Illustration: Betania Ruttia

Layout: Horacio Oteiza

Copy editing: Luis Pablo Alonzo Fulchi

DICIEMBRE 2020

Table of contents

1. General considerations

This work is based on the electronic voting system Vot.Ar of the MSA Group known as the «unique electronic ballot». The main references are its uses in Argentina, in the elections of 2015 in the Autonomous City of Buenos Aires (experience also analyzed in [1]), 2016 in the Province of Mendoza, 2017 in the Province of Corrientes and 2017 in the Province of Salta.

The company that owns the system, despite multiple requests from NGOs and communities of IT professionals, has never allowed a public and open inspection of its system, nor has it published parts of the software's source code.

Access to the equipment has been possible only in places of training for political parties or in places arranged for demonstrations of the system, but it has never been possible to carry out an actual audit of it.

Regarding the software, the portion that is distributed with the system startup DVD (including the voting and counting modules) has been leaked on several occasions, as was the module of transmission of results on one occasion[1,2].

Audits that have been published in districts where this voting system has been used have not provided any relevant technical details either, to the point of omitting the mention of certain components which have been found to be present in the systems in use in actual elections[3].

No technical specification or hardware specification for the voting, counting and transmission machines, as well as for the RFID chips used in ballots, records and credentials, has ever been published.

There is no information whatsoever about the software used in the servers that receive the polling data transmitted from the voting centers.

For these reasons, the current system may differ from the one described in this article, either due to the existence of elements not detected in the observations carried out or due to changes made by the company in the hardware or software over time.

1 https://github.com/prometheus-ar/vot.ar
2 https://www.telam.com.ar/notas/201708/199495-voto-electronico-codigo-salta.html
3 https://blog.smaldone.com.ar/2015/07/15/el-sistema-oculto-en-las-maquinas-de-vot-ar/

2. System description

2.1. Hardware

The voting machine is made up of two subsystems: one, which we will call main, based on an Intel processor; and another, which we will call secondary, based on an ARM processor (see image 1).

The main subsystem consists of a resistive-type touchscreen, a DVD reader (used for loading the operating system and the apps for voting, counting and the transmission of results), and external connectors for USB, Ethernet (network), VGA (video) and analog audio output. Internally, it has an Intel Celeron or Atom CPU (depending on the computer model) and 2 GB RAM memory.

The secondary subsystem consists of a thermal printer and an RFID reader/writer (following ISO-15693 standard). Both devices are connected to an ARM Atmel microcontroller, model AT91SAM7X256, which is in turn connected to the main subsystem through a USB port. The microcontroller is directly accessible through a JTAG connector.

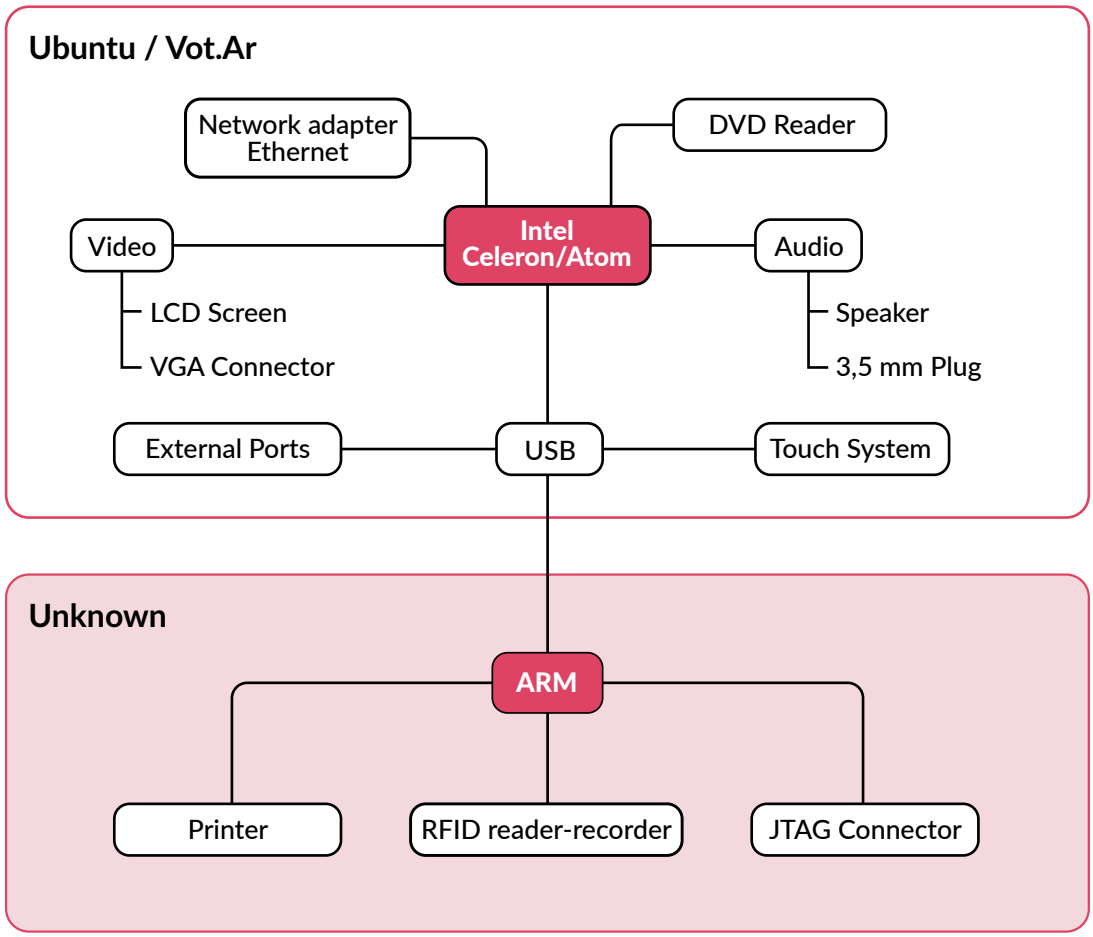


IMAGE 1: System architecture

The company has never provided a list of materials detailing the physical components used in the equipment and their specifications. For further details on the hardware used, see report [2], based on the equipment used in the City of Buenos Aires, Argentina, in July 2015.

IMAGE 2: External view of the voting machine

IMAGE 3: Bottom view (batteries and charger)

IMAGE 4: Top panel (ports)

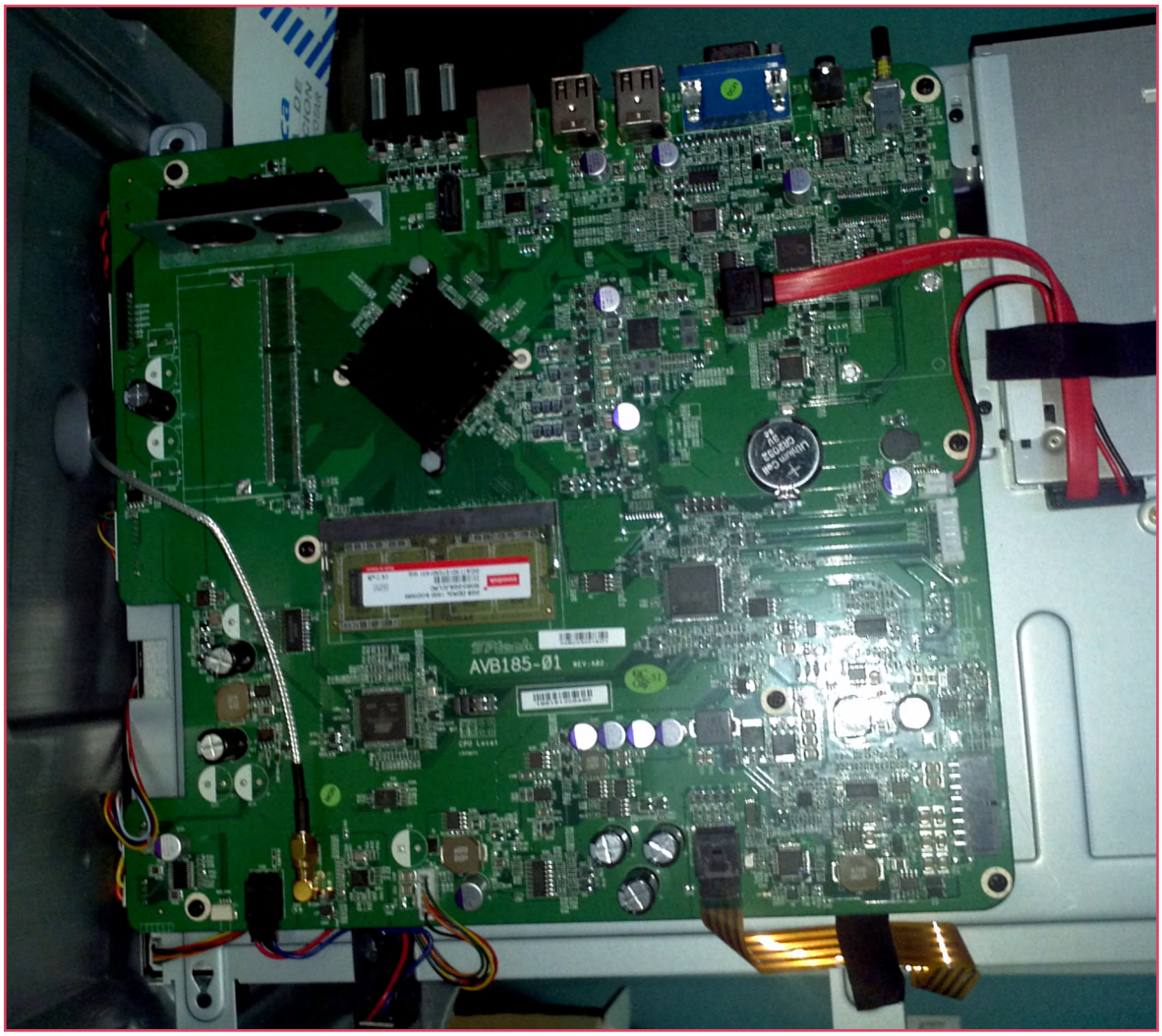


IMAGE 5: Motherboard

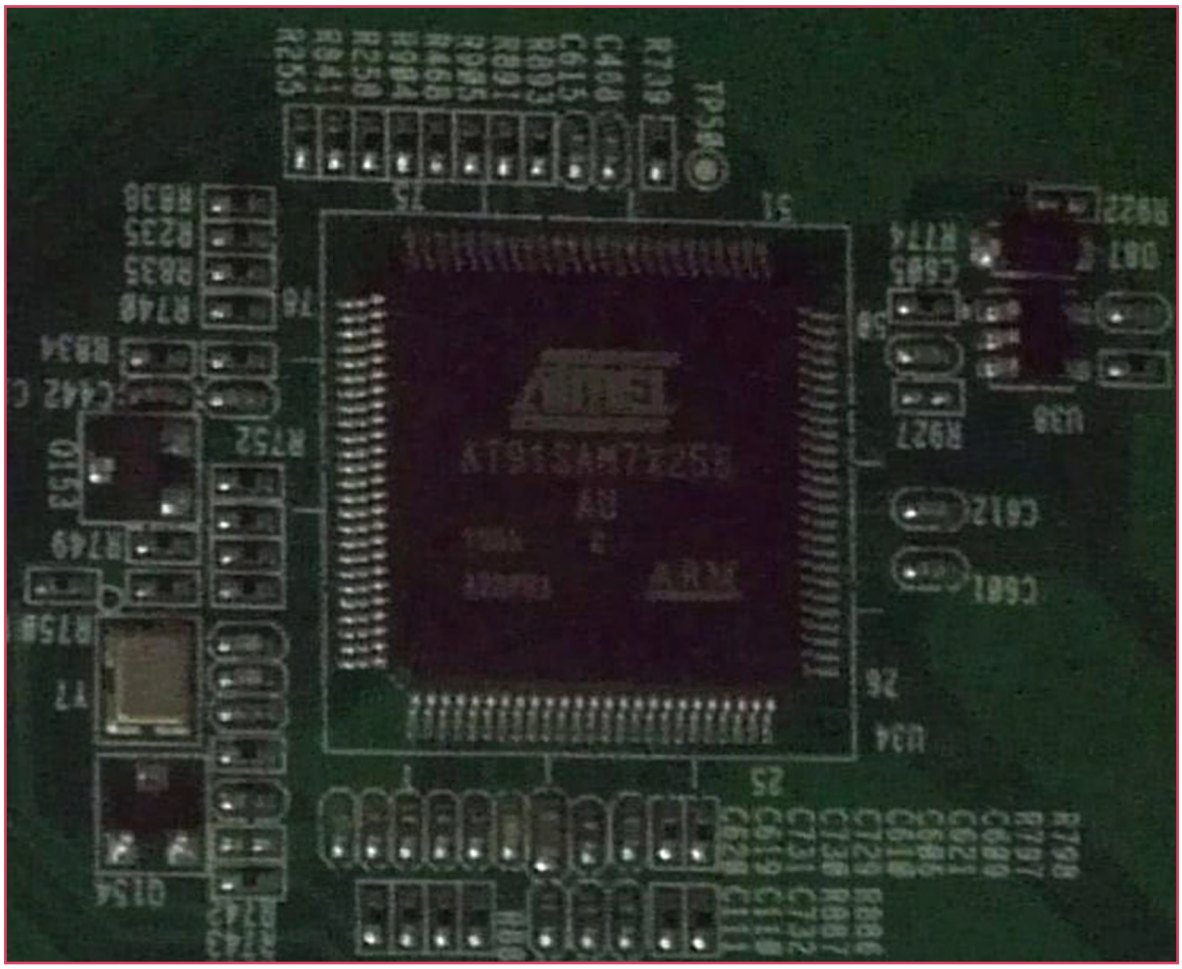


IMAGE 6: Atmel AT91SAM7X256 Microcontroller (never audited)

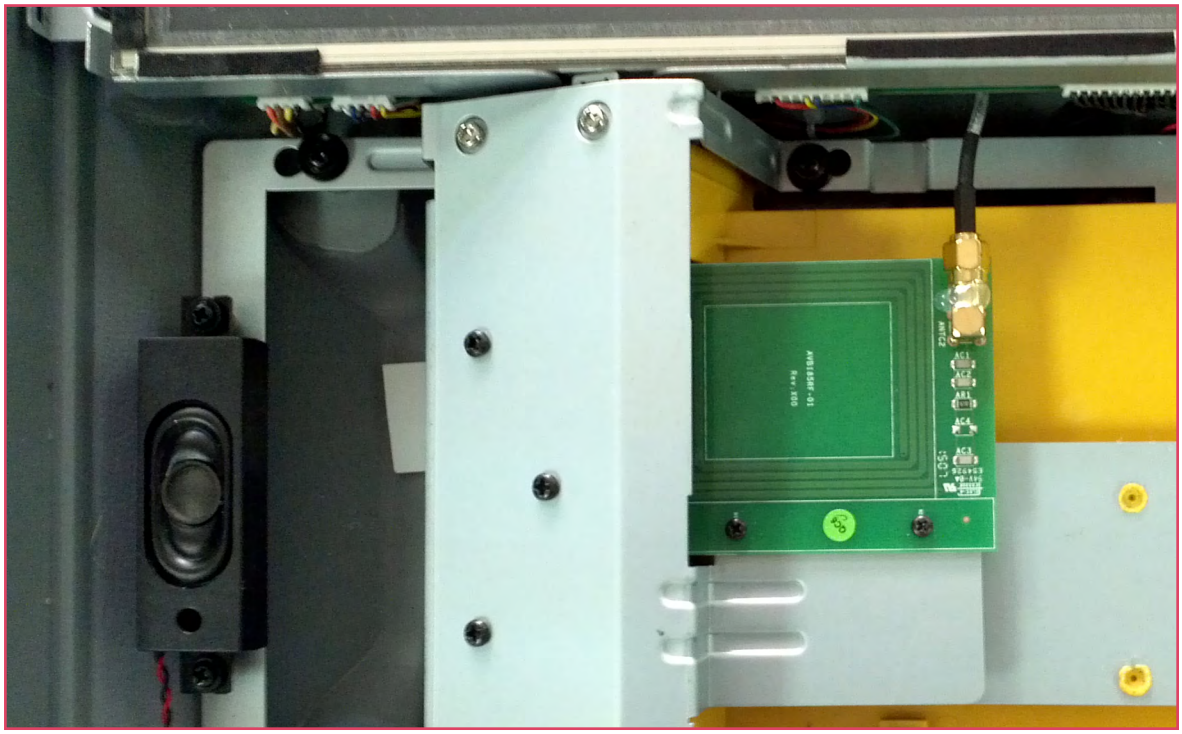


IMAGE 7: Thermal printer and RFID reader/writer

2.2. Software

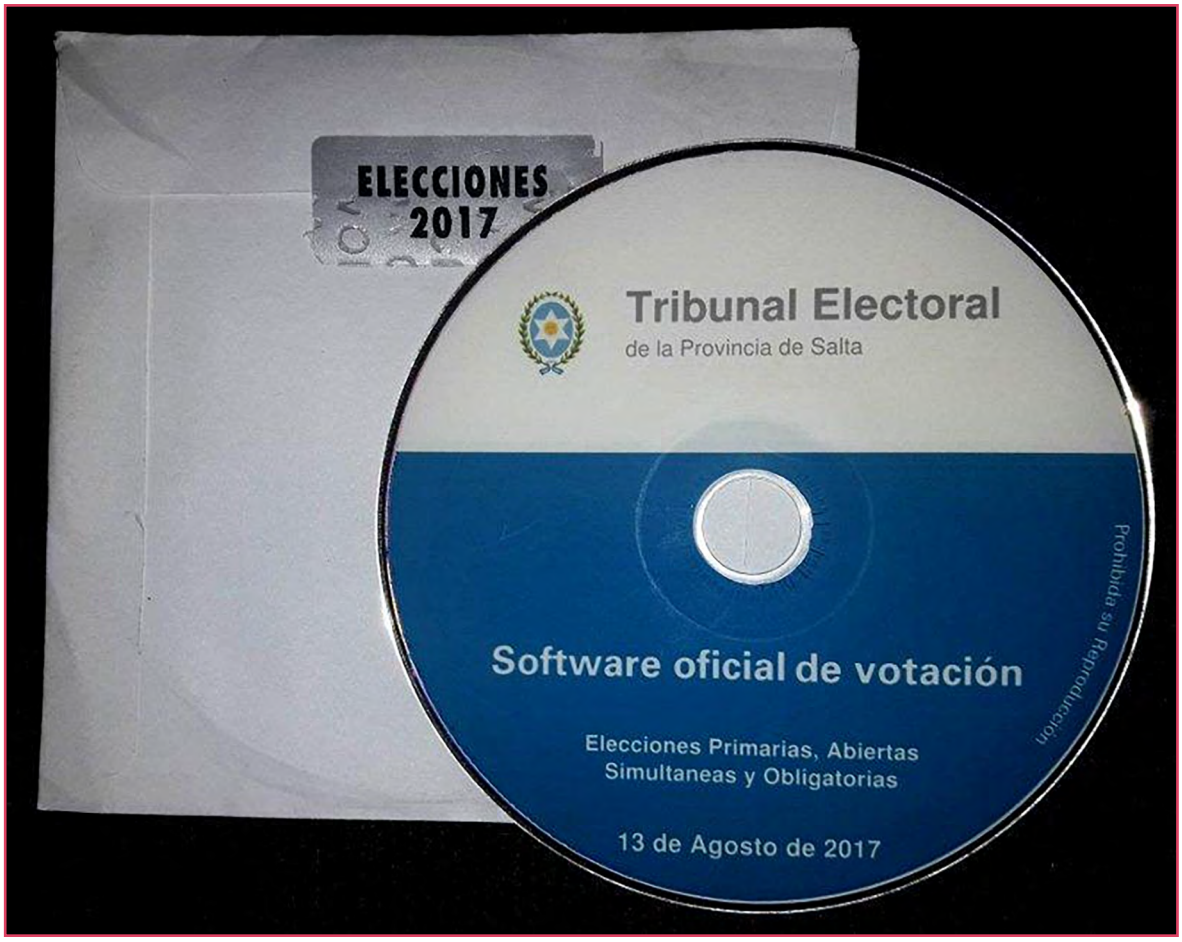


IMAGE 8: Software used in elections in the Province of Salta, Argentina

2.2.1. Voting and counting software

The DVD, which is delivered to the polling station chairman in a sealed envelope, contains a version of Ubuntu Linux OS and the software with the functionalities required for opening and closing the polling station, voting, and counting the votes. Regarding the operating system and the libraries used, these are standard ('off-the-shelf') versions, without any kind of customization for their specific use in a voting system.

2.2.2. Software for the transmission of results

The results transmission software, which also includes a version of the Ubuntu Linux OS, is contained on a DVD usually held by a technician from the supplier company.

2.2.3. Atmel microcontroller software

The software running on the Atmel microcontroller, developed in whole or in part by the MSA Group company, is unknown. It is responsible for the following functions:

1. Receiving the data to be printed on the paper ballot from the main subsystem, applying the corresponding format and sending it to the thermal printer.
2. Receiving the data to be stored on the RFID chip from the main subsystem and sending it to the RFID reader/writer.
3. Receiving the data read by the RFID reader/writer from a RFID chip and sending it to the main subsystem.

2.2.4. Software for receiving results

The software that receives the results (sent by the results transmission software from each voting center) is hosted on the company's servers. It has never been audited and it could never be publicly accessed. As a precedent, in the elections of the City of Buenos Aires, Argentina, in July 2015, an independent investigator detected and reported a serious vulnerability that could put the vote counting at risk[4]. A criminal complaint was filed against him and his house was raided, until the case was finally dismissed[5].

2.3. RFID chips

The RFID chips used in the ballots and credentials that we have been able to analyze are fabricated by NXP Semiconductors, models ICODE SLI SL2 ICS20[6] and ICODE SLIX SL2S2002[7], operating in accordance with ISO/IEC 15693 standard for vicinity cards, at a frequency of 13.56 MHz, with a range (according to the standard and according to the manufacturer) of about 5 ft (1.5 meters).

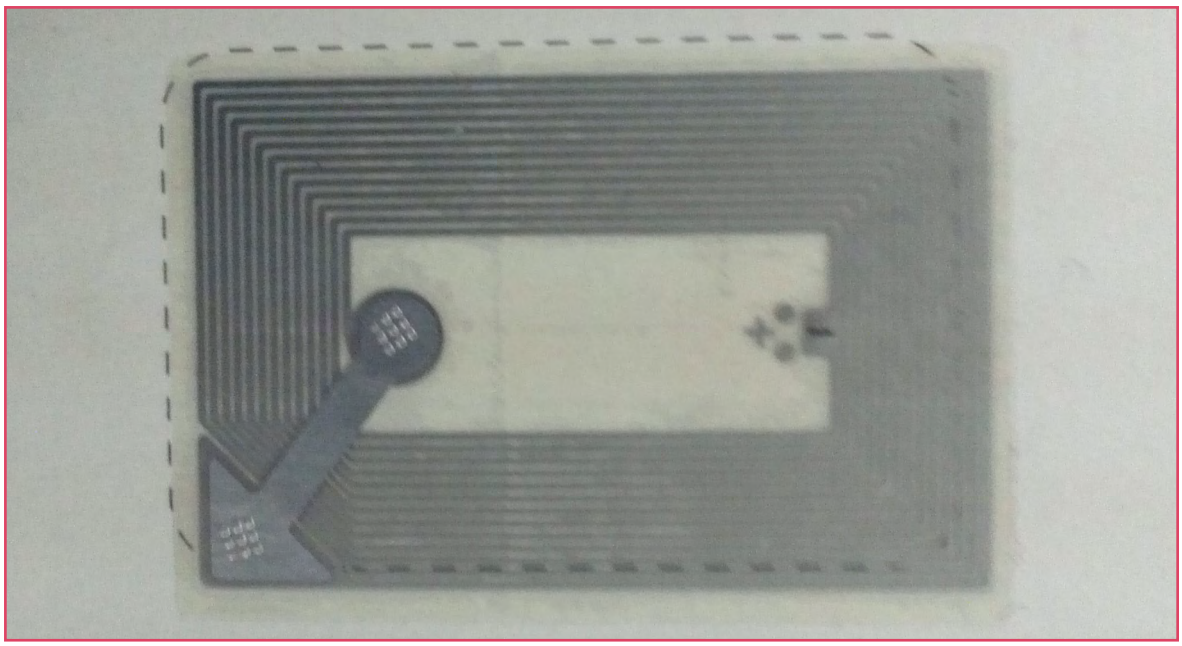


IMAGE 9: RFID chip embedded in a ballot

4 https://blog.smaldone.com.ar/2016/05/03/el-dia-que-el-sistema-de-voto-electronico-vot-ar-fue-vulnerado/
5 https://www.lanacion.com.ar/tecnologia/sobreseyeron-al-programador-que-revelo-fallas-en-el-sistema-de-boleta-unica-electronica-nid1924088/
6 https://www.nxp.com/docs/en/data-sheet/058031.pdf
7 https://www.nxp.com/docs/en/data-sheet/SL2S2002_SL2S2102.pdf

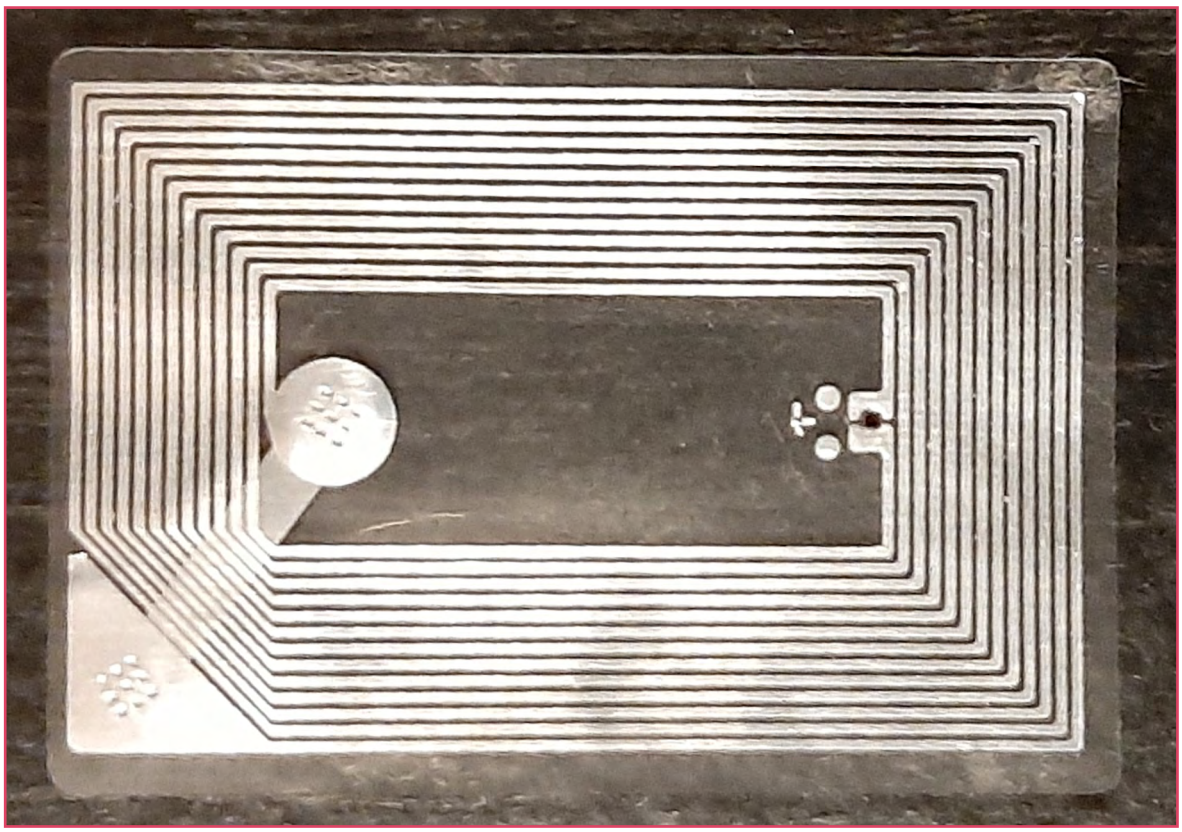


IMAGE 10: RFID chip

2.3.1. General characteristics

A distinctive feature of this technology is that each RFID chip has a unique unchangeable number called 'UID', set by the manufacturer. However, there are chips with programmable UID available[8], which could be used in various types of attacks.

ICODE SLI and SLIX chips do not feature authentication, authorization or encryption mechanisms, which means that they can be read or written using any RFID/NFC device supporting ISO 15693 standard, beyond the voting computers used in the system, without requiring any type of password.

2.3.2. Credentials

Each technician of the owner company, as well as each polling station chairman, has a credential to authenticate himself before the system, a requirement to access the functionalities reserved for each type of user. Each credential has an RFID chip with a special value stored in its register (which indicates the type of user, differentiating them from each other and also from the voting ballots). For more details, see "B. 1. Data structure" in [3].

8 https://lab401.com/products/icode-sli-slix-compatible-uid-modifiable

2.3.3. Polling station records

The opening, closing and voting totals records are generated using ballots that also contain an RFID chip and have a distinctive color and text.

2.3.4. Ballots

IMAGE 11: Image 11: Ballot (front and back)

Each voting ballot incorporates an RFID chip of the type already described, generally with all its registers set to zero (0), except the last one that may contain the value 'W_OK'. In no voting instance carried out in Argentina using this system has any encryption mechanism been used, so the information of each ballot is stored in the chips in the form of 'plain text', legible, reproducible and modifiable by anyone with a suitable device.

The RFID chips used have a mechanism that allows, once a piece of information has been recorded, to block it in order to prevent its subsequent modification. In the analyzed versions of the voting software there is an option that makes use of this mechanism to block the content of the vote once it has been recorded on the chip, but this option can be deactivated by modifying the source code, which would allow the stored vote to be altered at a later time.

With regard to the legibility and reproducibility of the vote contained in the chip, encryption functions were incorporated in the last analyzed version of the software (using as key the UID that identifies each chip and the PIN of the polling station chairman). In none of the Argentine elections where the system has been used has this mechanism been activated.

This, we assume, is due to the fact that by using the polling station's PIN in the encryption, the votes cast by the voters at a given polling station could only be counted later by the same issuing machine, thus leaving each voting computer linked to a particular station. Thus, in the event of the failure of a machine, another one could not be shared among voters from different polling stations, significantly increasing the number of machines required in each voting center.

3. Principles of use

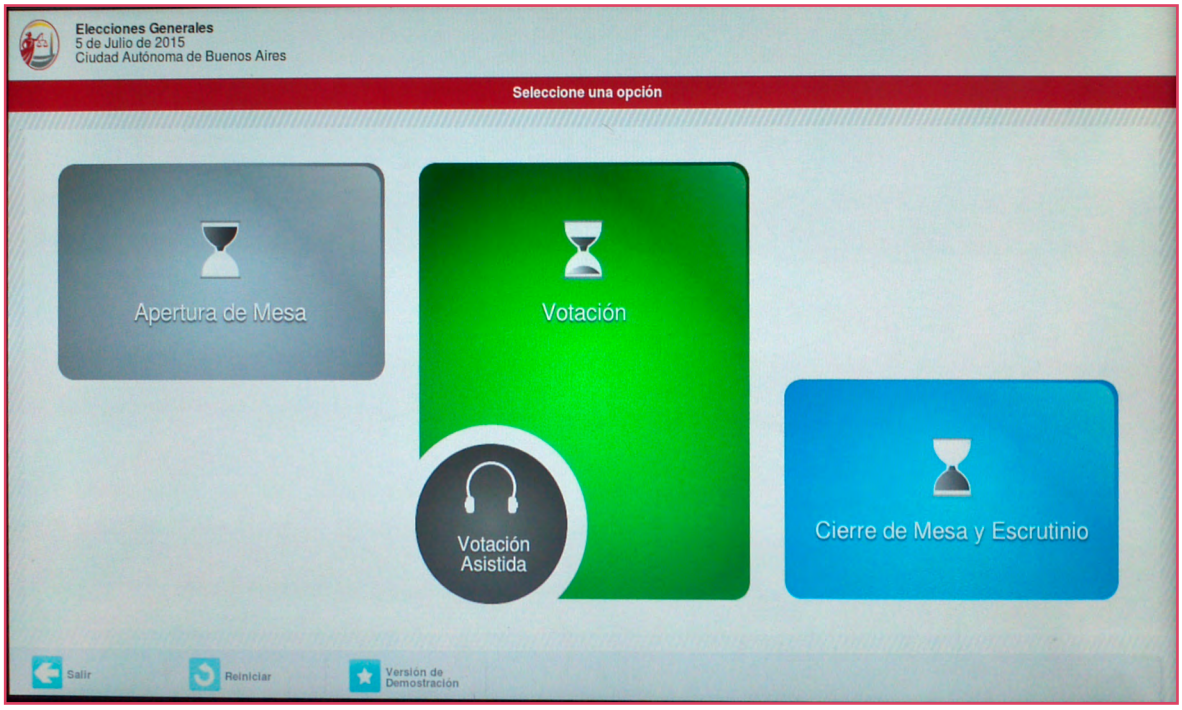


IMAGE 12: Main screen of the voting and counting system

3.1. Polling station opening

Once the voting machine is set up in the chosen place and connected to the power supply, the DVD with the voting and counting software is inserted. When the machine is turned on, and after the BIOS startup screen, it will first load the operating system and then finally the voting application.

Once the system is loaded, the polling station chairman must proceed to opening the voting session. To do this, he selects the option “Voting Opening”, brings his credential to the RFID reader and enters a PIN code, both items delivered to him in a sealed envelope along with the polling station material.

Then he must proceed to issue the opening records. A special ballot is introduced, in which the names of the election officials and party representatives will be printed and recorded.

This ballot will be used at the end of the voting day to close the session. It may also be used in case of having to restart the voting machine or replace it with a new one.

After issuing the opening records, the chairman will select the “Voting” option and the system will be ready for the casting of votes.

3.2. Voting

Once a voter has been identified, he receives a blank electronic ballot from the chairman. Before delivering the ballot, the chairman tears off and keeps the top half of the ballot die cut tag.

The voter then goes to the voting machine, inserts the ballot in the slot provided for this purpose and the system proceeds to show him the electoral offer. In the event of any anomaly in the chip, the machine will eject the ballot, in which case the voter must ask for a new one.

After choosing his vote, the voter must confirm it. Immediately afterwards, the RFID reader/writer writes the data to the chip, the printer pulls the ballot in, prints the vote and then ejects it.

Once this is completed, the voter may bring the RFID chip to the reader, in which case the machine will read it and display the data obtained on the screen.

Before returning to the election officials table, the voter must fold the ballot in half, matching the metal tag on one end with the RFID chip on the other. The chairman will then detach the lower half of the ballot die cut tag and verify that it matches the upper half already in his possession.

Finally, the ballot is deposited by the voter into the ballot box.

3.3. Polling station closure

At the end of the voting day, the polling station chairman brings his credential to the RFID reader, enters his PIN and then chooses the option “Voting Closure and Ballot Counting”. He must insert the special ballot where the voting closing time will be printed and recorded.

3.4. Vote counting

To start counting the ballots, the closing records must be brought to the RFID reader/writer, thus switching the software to ‘ballot counting mode’. Then, the RFID chip of each voting ballot is read, and the machine counts the data, also showing the details of each ballot on the screen.

When the counting is over, a special ballot called ‘polling station results record’ is issued, which contains the totals both printed on the paper and recorded on its RFID chip. At least in the analyzed system, no instance of manual correction of the results is expected to happen.

3.5. Transmission of results

To transmit the results of a polling station, a company employee starts the voting machine using a special DVD that contains the software used for this purpose. Once the machine is connected to the Internet (using an Ethernet network connection, a 4G modem or some other connectivity technology), it proceeds to read the RFID chip of each of the polling station records and, after the electoral authorities see and verify the data being read, it is sent to a central server of the company.

4. Attacks

This section describes some attacks that have been identified as possible (and in many cases tested at a 'proof of concept' level) on the Vot.Ar. system. For this analysis, the following actors have been considered as possible attackers:

- Voters
- Election officials
- Party representatives
- Employees of the supplier company
- Technicians hired for the elections
- Suppliers of the supplier company (and by transitivity, suppliers of those)

4.1. Credential spoofing

4.1.1. Technician credential

The technician credential allows access to some system configuration options. These include, among others, adjusting the print quality or being able to eject the DVD. To generate a technician credential, it suffices to have an RFID chip with the value 0x0002 stored in bytes 2 and 3.

Mitigation: There is no way to mitigate this attack without a redesign of the authentication system.

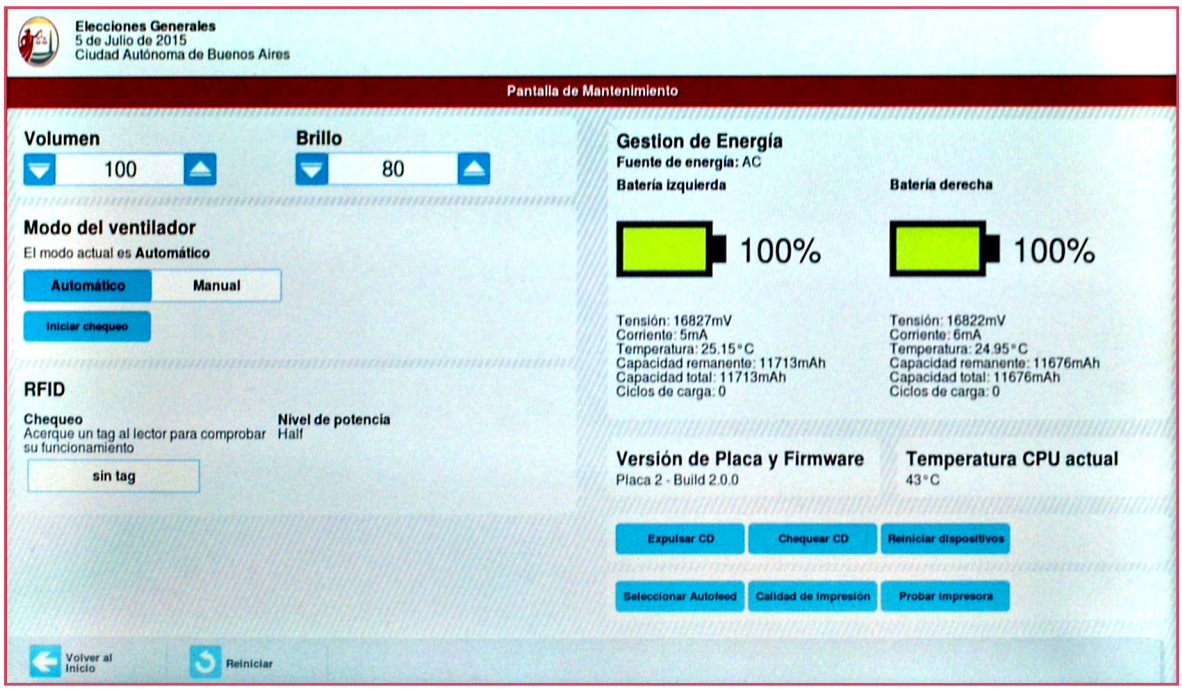


IMAGE 13: Maintenance mode (accessible through a technician credential)

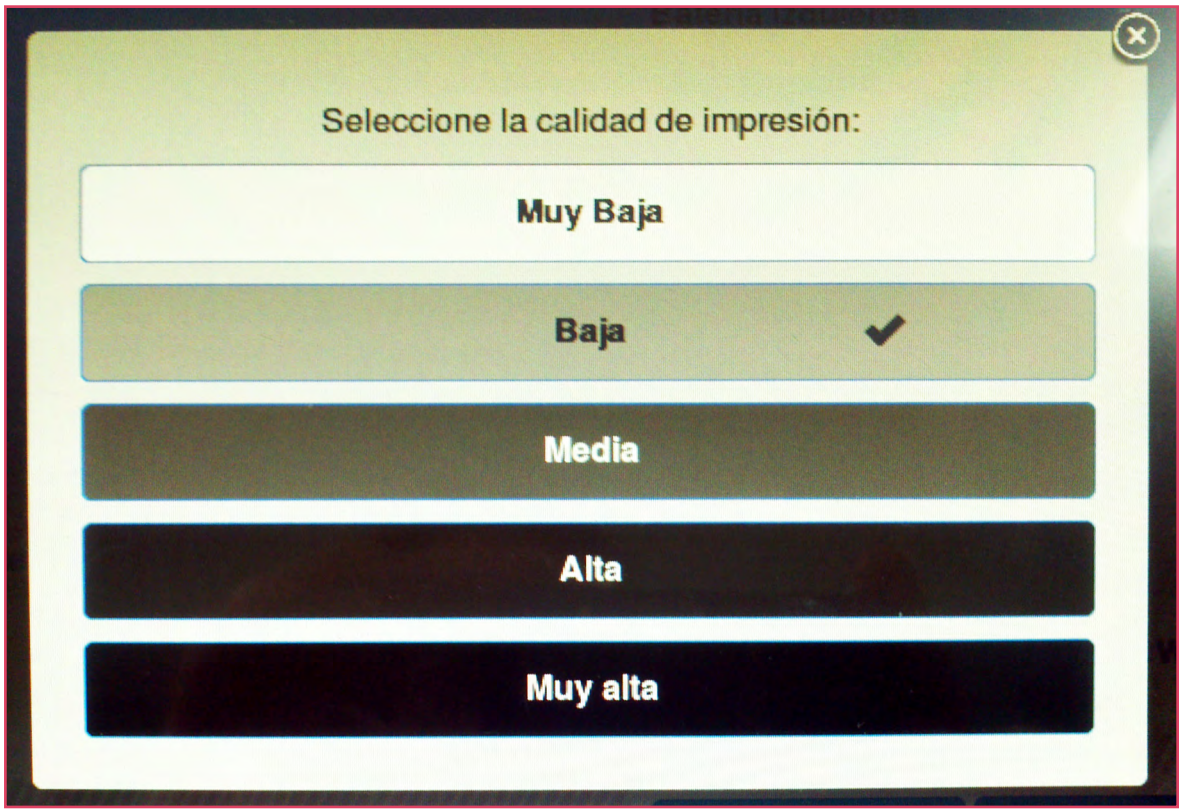


IMAGE 14: Selecting the print quality

4.1.2. Polling station chairman's credential and opening record

The polling station chairman's credential allows the issuance of the opening and closing records, as well as the enabling of the voting mode. It must be accompanied by a PIN, which is also delivered in a sealed envelope. This credential can be generated using an RFID chip with the value 0x0003 stored in bytes 2 and 3.

All the functions of the chairman can be carried out without having the corresponding credential and PIN, by having instead a valid voting opening record. To generate an opening record, it suffices to record the value 0x0005 in bytes 2 and 3 on an RFID chip. When an opening record is brought to the RFID reader, neither the credential nor the PIN of the chairman are requested.

Mitigation: There is no way to mitigate this attack without a redesign of the authentication system.

4.2. Duplication of polling records

Both the opening and closing records can be generated by writing certain values on an RFID chip, since the system does not use, at least in the versions analyzed, any encryption function or mechanism to verify their authenticity. A regular voting ballot can be used for this, since they all use the same type of chip.

Mitigation: There is no way to mitigate this attack without a redesign of the record generating system.

4.3. Chip ID

As mentioned above, each RFID chip has a unique identifier (UID). This results in each voting ballot being numbered in a way that is not visible to the human eye, but can be detected by various devices. If it could be determined which UID corresponds to the chip of the ballot given to a certain voter, it could then be determined how he voted, thus breaking the secret.

Mitigation: One way to partially mitigate this attack is to allow the voter to choose an arbitrary ballot, taking care that there is no device in the vicinity of the table capable of reading the UID of the ballot's RFID chip.

4.4. Chip burning

RFID chips are passive, that is, they do not possess their own source of energy. They obtain the electrical energy necessary for their operation from the radio signal received from the RFID reader/writer. If too strong a signal is generated, the chip can be overloaded and burned. In experiments carried out with devices that generate low intensity electromagnetic pulses (see image 15), it has been possible to burn the RFID chips used in this system, from a distance of about an inch[9]. Using greater power, the same attack can be carried out from a distance sufficient to burn all the chips of the ballots deposited in a ballot box, preventing

9 https://www.youtube.com/watch?v=DgXYw9ZDxns

their automated counting. Likewise, it could burn all the chips of the ballots in the possession of the polling station chairman, thus preventing the vote itself.

Mitigation: To mitigate this attack, the blank ballots can be deposited in a container that generates a 'Faraday cage' effect. The ballot box should also have this type of protection.

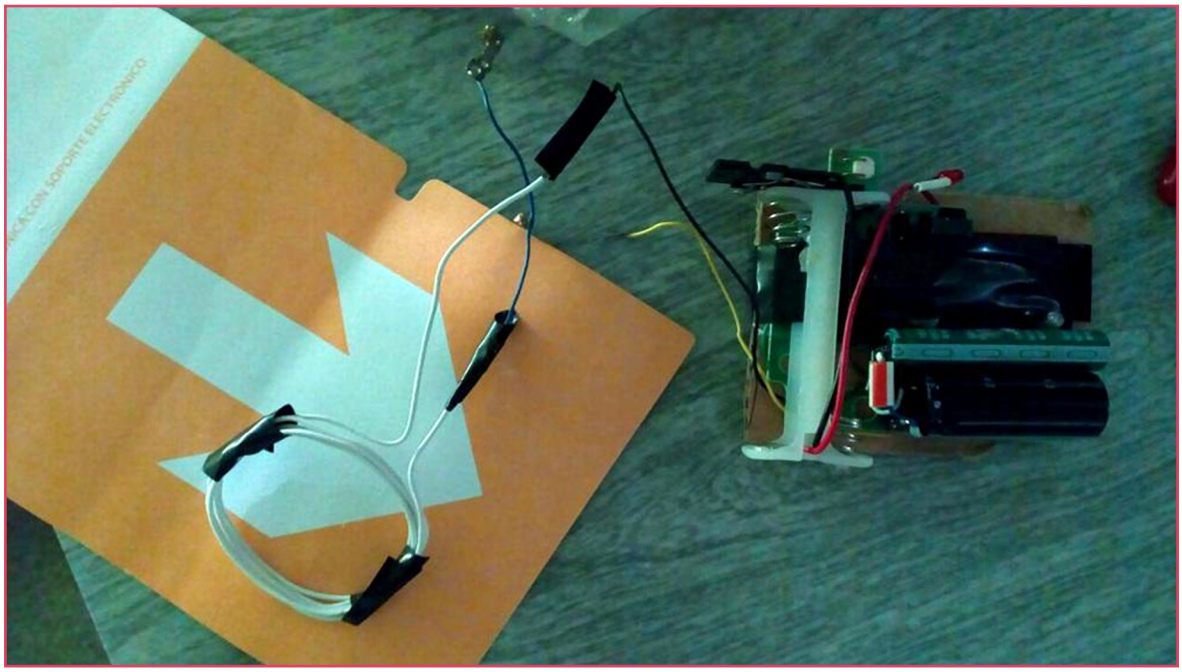


IMAGE 15: RFID chip burner

4.5. Software manipulation

In the last versions analyzed, the Vot.Ar system has incorporated some verification functions at system boot (secure boot), but there are still ways to alter the software. This could be done on the DVD used to distribute it to each voting station, as well as during run-time (after the system has started). Furthermore, since the hardware used does not have a 'secure element', the 'secure boot' mechanism can be manipulated by someone with physical access to the machines. On the other hand, the software that runs on the Atmel microcontroller, responsible for printing the ballots and reading/writing its RFID chips, can be modified by accessing the JTAG interface provided for this purpose.

It is possible to make malicious changes to software that are undetectable in 'black-box' testing, that is, they cannot be discovered by carrying out use tests. This can be achieved by allowing the system to work in a lawful way until some external event occurs as a signal (such as the reading of an RFID chip with certain values, or a series of clicks on certain areas of the screen), enabling the malicious behavior.

Furthermore, as a standard software distribution without specific customization is used (Ubuntu Linux), there are a large number of software components that are not under the control of the system provider company. Therefore, in the event of the detection and pub-

lication of security problems in any of these components in the days prior to the election, it would not be possible to upgrade them.

4.5.1. Vote issuing

By manipulating the vote issuance software, various forms of fraud can be implemented. The simplest one is to make it difficult to choose a candidate or party, for example by making it tend to appear in less prominent places on the screen or by simulating selection errors attributable to the limitations of the touch screen.

In the presentation made by the author before the Argentine Senate, an example was provided of an attack on the Atmel microcontroller software[10] that would allow the voter's selection to be replaced by an arbitrary one, in a way that could go unnoticed by the voter or, in case of being detected, could be attributed to a voter error or discarded as a false complaint.

It may also happen that a voter declares that he cast a vote for one candidate but the result is a printed vote in favor of another one. In this case, the situation may be adjudicated to a failure (intentional or not) of the system. The veracity of the voter's statement would be unverifiable, but it would generate at least a delay for the rest of the voters and, if it is done in a generalized way in many polling stations, it could possibly cause some kind of turmoil[11].

The fact that the system keeps two records of the vote cast, one printed on the paper and the other recorded on the chip, enables the software to be modified so that both do not coincide, and that one or both of them do not coincide with the intention of the voter. This would allow a variety of attacks that would facilitate the commission of fraud in various ways. In addition, the verification of the vote stored in the RFID chip to contrast it with what is printed on the paper is carried out by the same computer with which it was cast, rendering the checking option completely useless.

Mitigation: To reduce the risk of these types of attacks, the DVDs used in each voting machine should be verified, computing the corresponding hashes to verify that they coincide with those previously registered by the electoral authority. The integrity of the code stored in the Atmel microcontroller should also be verified, requiring the removal of the cable that allows external access to the JTAG port (see image 16). In both cases, additionally, the publication of the source code of the software and the detailed design of the hardware are essential. A second device should also be incorporated, independent of the voting machine, so that the voter could verify the data stored in the RFID chip. During the counting of the votes, special attention must be paid to ensuring that the content read from each RFID chip corresponds to what is printed on each paper ballot.

10 https://www.youtube.com/watch?v=rd1aOFXZl5Q
11 https://www.lmneuquen.com/escandalo-fraude-san-luis-una-maquina-emitia-votos-el-partido-del-intendente-n570919

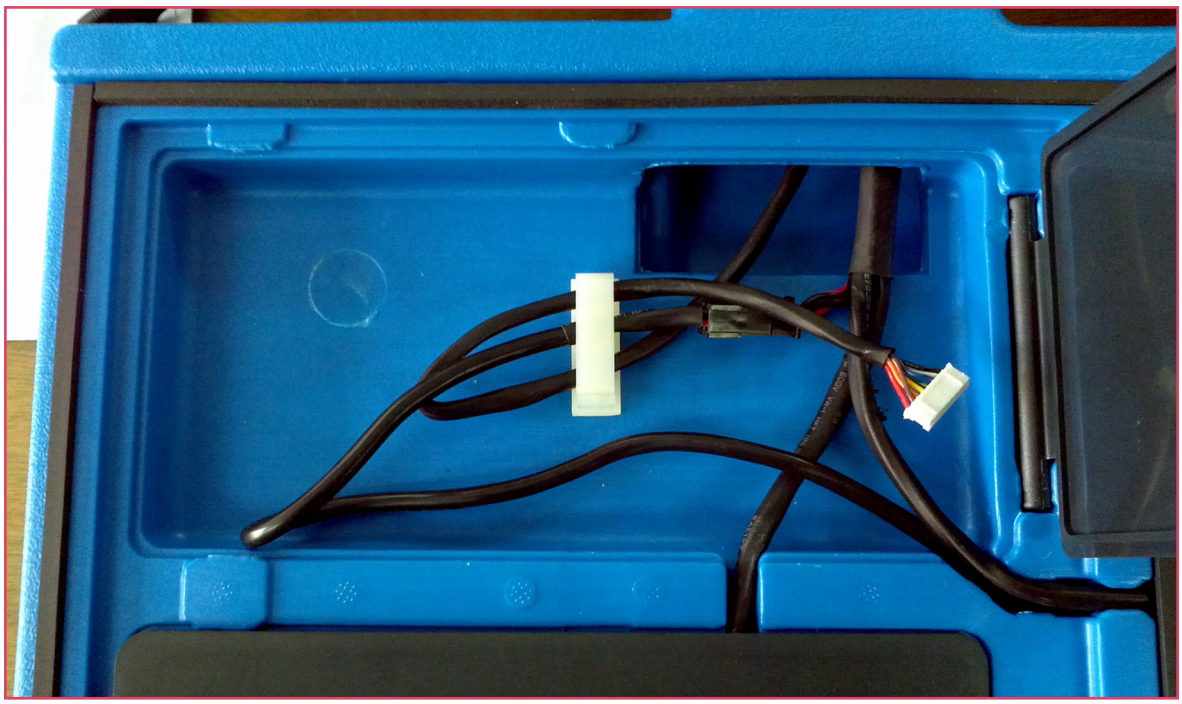


IMAGE 16: JTAG cable at the base of the machine

4.5.2. Vote counting

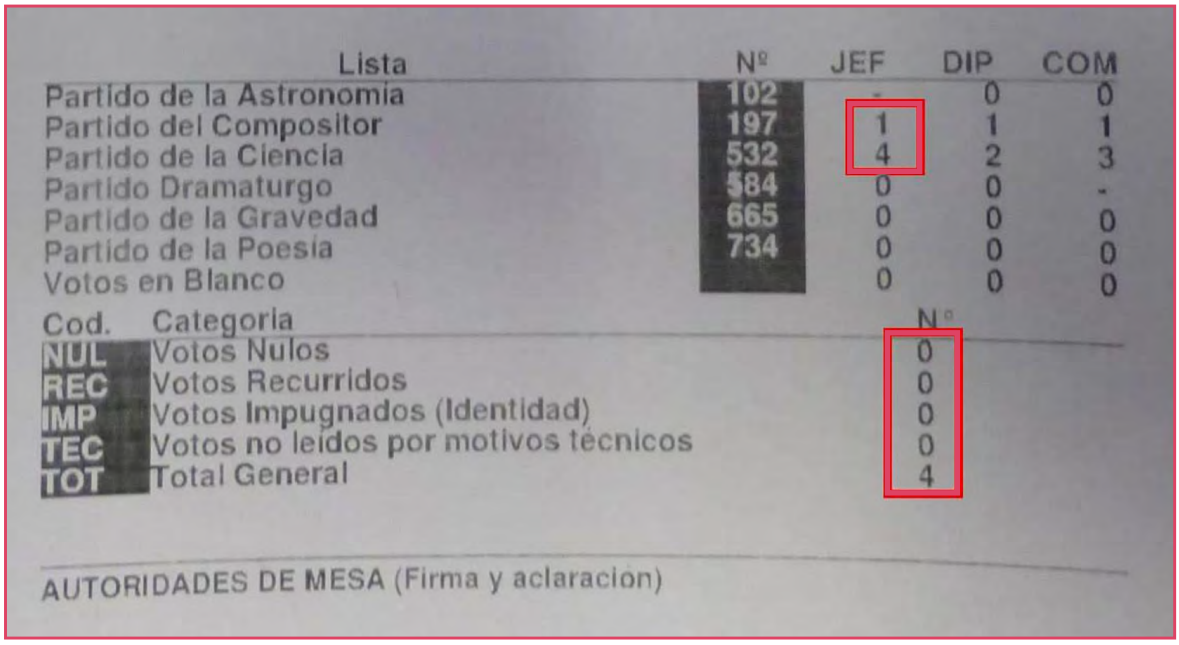
Modifying the vote counting software may allow the vote count to be altered. In the experiences of several Argentine elections, it has been appreciated that polling station chairmen and party representatives tend to trust the computer system and do not carry out an independent count to corroborate the results.

In 2015, independent researchers found an error in the counting system that allowed an RFID chip to store more than one vote, and the system would count them as legitimate. If the count is not controlled, the situation could go unnoticed, resulting in a greater number of votes than the ones actually cast. This attack, known as 'multi-vote' (see image 17), had not been detected by any audit carried out up to that time (at least two from the National University of Salta and one from the National University of Buenos Aires)[12]. The existence of other such errors, as well as the malicious introduction of similar behavior, cannot be ruled out if the scanning software is altered by some malicious maneuver.

Mitigation: The polling station chairman and party representatives must keep an independent count, verifying that the content of each RFID chip matches the data printed on the ballot paper and leaving a written record of any discrepancies.

12 https://blog.smaldone.com.ar/2015/09/04/ataque-multivoto-en-el-sistema-vot-ar/

IMAGE 17: 'Multi-vote' attack



Lista	Nº	JEF	DIP	COM
Partido de la Astronomía	102	-	0	0
Partido del Compositor	197	1	1	1
Partido de la Ciencia	532	4	2	3
Partido Dramaturgo	584	0	0	-
Partido de la Gravedad	665	0	0	0
Partido de la Poesía	734	0	0	0
Votos en Blanco		0	0	0

Cod.	Categoría	Nº
NUL	Votos Nulos	0
REC	Votos Recurridos	0
IMP	Votos Impugnados (Identidad)	0
TEC	Votos no leídos por motivos técnicos	0
TOT	Total General	4

AUTORIDADES DE MESA (Firma y aclaración)

IMAGE 18: Inconsistent record as a result of the 'multi-vote' attack

4.6. Filling of ballot boxes

The system closing record does not include any information on the number of votes cast during the day. This is because in the middle of the voting day the system may be restarted or the voting machine may be replaced by another one. During the vote counting, the system counts each ballot and at the end reports the total number in the polling station results record.

In the experience of several Argentine elections, we have observed that the polling station authorities do not contrast the number of votes counted by the system with the number of votes cast, since the system does not allow the entry of the latter data and there is no manually prepared document.

On the other hand, the voting ballot does not incorporate any security measure to guarantee that it corresponds to the polling station where it was supposedly cast (beyond the die cut tag used during the casting of the vote, which is completely detached from the ballot before it is inserted in the ballot box).

After casting their vote using the system, the voters return to the authorities table with the ballot folded and held in their hands. At no time does the voter detach himself from it, or unfold it, so it is impossible at first glance to determine whether he has a single ballot or several. In this way, a voter could, for example, introduce two ballots in the ballot box: one validly issued on the spot and another one previously printed and delivered to them[13]. At the time of counting, it would be impossible to differentiate them and, if the number of ballots were not also contrasted with the number of voters, the situation would go completely unnoticed.

13 https://www.youtube.com/watch?v=fBUe3fKMSFQ

Mitigation: A count should be kept of the number of voters who cast their vote, and a manual report should be made that reflects this figure. The ballot should include some physical security measure that allows determining whether it is a valid vote or not (for example, the signature of the polling station chairman and the representatives, a stamp with the number of the polling station, etc.).

4.7. Adding wrongful votes

Using RFID chips with programmable UID (currently available on the market) and a reader/writer device, the counting could be altered, 'injecting' false votes into the system. An RFID chip emulator, such as a Proxmark3[14], ChameleonMini[15] or a similar device, could also be used for this purpose to add wrongful votes.

Mitigation: Properly supervise the vote counting, to avoid false votes being counted.

4.8. Remote chip reading

RFID technology is based on the transmission of information using radio waves. According to the manufacturer's specifications, the chips used in this system can be read up to a distance of approximately 5 ft (depending on the size and power of the antenna).

4.8.1. While casting the vote

Due to the nature of the radio waves emitted by the RFID recorder, and regardless of the technical specifications of the chip, they are perceptible from a distance much greater than 5 ft. This has been demonstrated in laboratory tests and publicly exposed in the Argentine Senate[16].

The attack consists of analyzing the radio waves received by a receiver at a frequency of 13.54 MHz (short wave) and analyzing the sound. Using a smartphone with NFC (with lower power than the RFID reader/writer used in the voting machines) and featuring a recording app[17], a home radio receiver connected to a notebook, and detection software[18], it was possible to differentiate two different bit patterns (data) with 100% accuracy from 6.56 ft (2 m) away and more than 80% from 8.86 ft (2.70 m). This could make it possible to determine whether or not a person votes for a particular political party or candidate.

These types of attacks, known as 'side-channel', could also be carried out by analyzing other variables, such as electricity consumption, noise level, electromagnetic emission from the components (Van Eck radiation), etc. These techniques have been used in the past to break secrecy in electronic voting systems in the Netherlands[19] and Brazil[20].

---

14 https://hackerwarehouse.com/product/proxmark3-rdv4-kit/
15 https://lab401.com/products/proxgrind-chameleon-mini-revg
16 https://www.youtube.com/watch?v=yrFSQBj1Emo
17 https://github.com/tristangrimaux/Nemo
18 https://github.com/ortegaalfredo/nfcread
19 https://www.youtube.com/watch?v=hwz1BLRgTg0
20 http://web.archive.org/web/20130917064411/http:/idgnow.uol.com.br/seguranca/2009/11/20/perito-quebra-sigilo-eleitoral-e-descobre-voto-de-eleitores-na-urna-eletronica/

Mitigation: With the current system design, there is no way to fully mitigate this attack. To reduce the risk, the voting machine's RFID reader/writer must be set to its minimum power (option provided in the source code of the voting software).

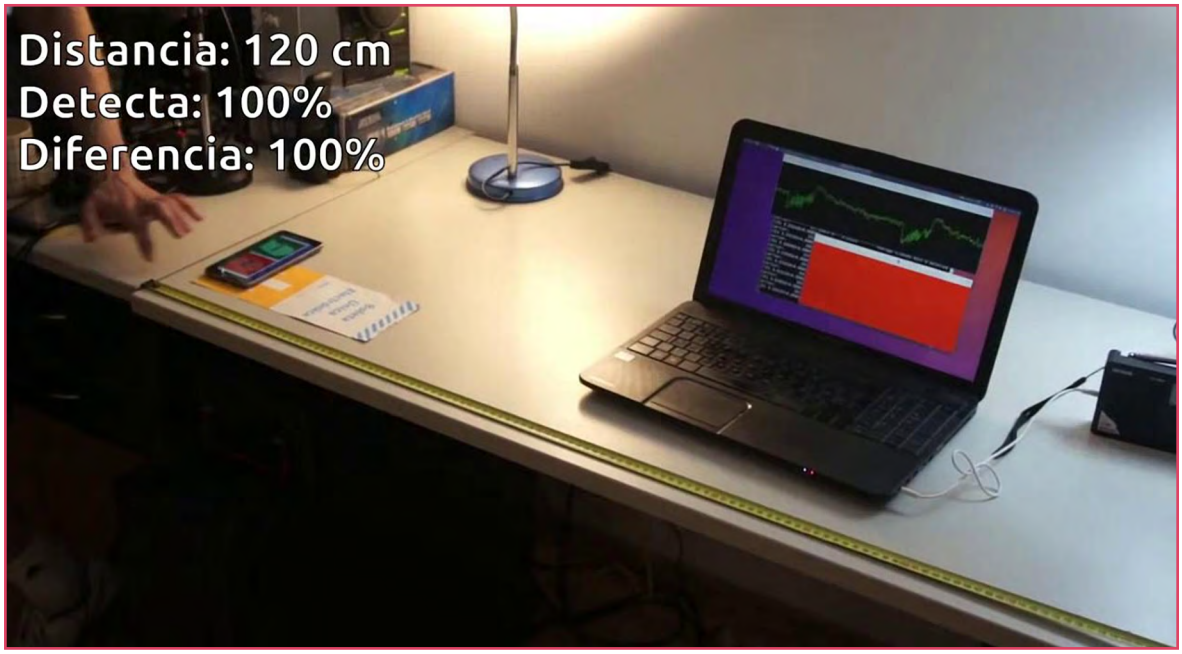


IMAGE 19: Write differentiation on RFID chips

4.8.2. After casting the vote

As mentioned in 2.3.4, votes are recorded on the chips without applying any encryption mechanism. Therefore, its content can be read using any RFID or NFC reader (such as the one included in many smartphones). In 2015, an app called 'Digital Pointer'[21] was developed to demonstrate how by using a smartphone, possibly hidden among the voter's clothes, a person could show to a third party who he voted for, creating the possibility of buying votes. This app was also presented in the Argentine Chamber of Deputies in August 2016[22]. The same attack could be achieved using a device manufactured for this purpose, at a significantly lower cost than a smartphone and with smaller dimensions.

Mitigation: Enable vote encryption features already included in the 2017 version of the software.

21 https://blog.smaldone.com.ar/2015/09/03/comprando-votos-con-la-boleta-unica-electronica/
22 https://www.youtube.com/watch?v=XA3JZ2HWQuA

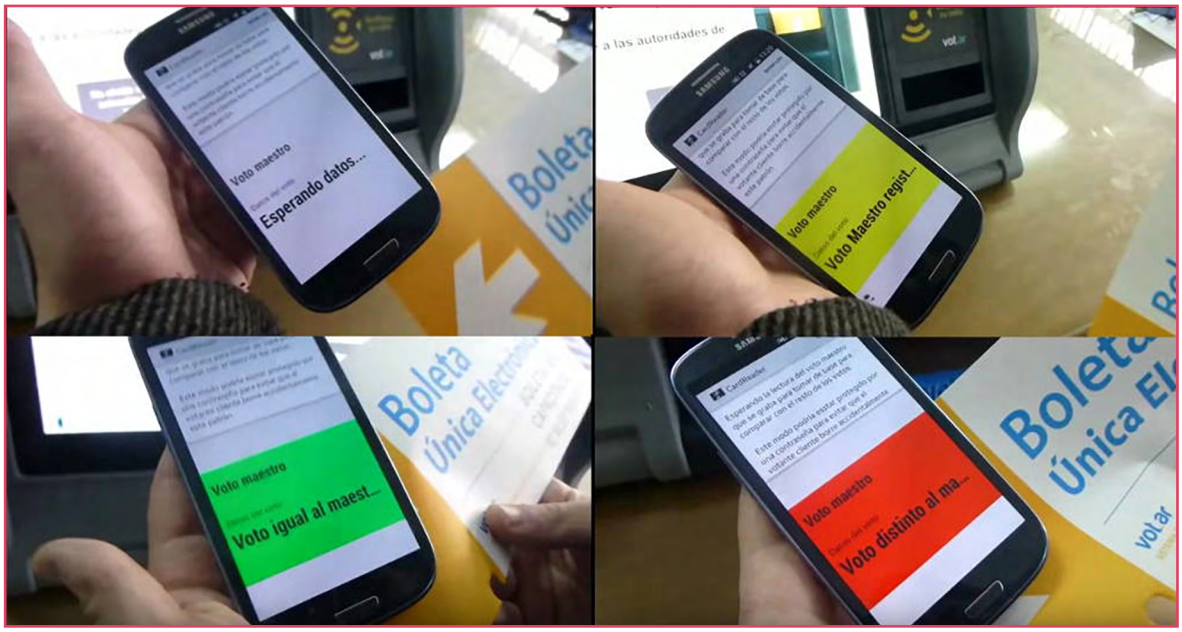


IMAGE 20: Image 20: 'Digital pointer' app

4.8.3. Inside the closed ballot box

According to [4], the system was originally designed so that votes could be counted remotely, without the need to open the ballot box:

> "The vote count does not require the opening of the ballot box. This is possible since all EVB [Electronic Voting Ballots] have their own chip (TAG RFiD) that can be read by the interrogation of a simple RF antenna from the outside [...]. According to the company, this is one of the new security elements incorporated, in that only the voter touches his ballot. The ballot box could be opened in a case of extreme necessity and only by the competent authority."

Furthermore, the patent obtained in Argentina by the MSA Group company in 2007[23] recognizes that:

> "...another goal of the present invention is to provide means to ensure the secrecy of the vote in the electronic voting ballot, among which is the reading of all the TAG RFIDs inside the Ballot Box, without having to open it, avoiding all manual contact with the ballots."

Mitigation: Although in later versions of the system a metal sheet was added to the ballot, which when folded coincides with the RFID chip and would absorb radio waves making it impossible to be read, such a mechanism only works if the separation between the two elements is minimal (less than 0.2 in, or 5 mm). A possible way to mitigate this type of attack would be to add some kind of adhesive to the ends of the ballot that would allow it to be firmly folded. The ballot box could also have some kind of covering that creates a 'Faraday cage' effect.

23 https://blog.smaldone.com.ar/files/rfid/memoria.descriptiva.patente.votoelectronico.pdf

4.9. Vandalism

4.9.1. Voting machines

There are multiple ways to affect the normal operation of the voting machines, from damage caused to the touch screen with a sharp element, to the injection of liquid through some of the ports that are easily accessible from the outside. Attacks can also be carried out on the electrical supply system, limiting the operation of the machines only to the autonomy time provided by the batteries. Attacks on the thermal printer have been seen in Argentine elections, introducing chewing gum or cigarette butts in order to render them useless.

4.9.2. Ballots and records

In addition to the electromagnetic pulse attack described in 4.4, a chip can also be physically destroyed, using a sharp-pointed element such as a pen or a needle. This, if done after casting the vote and before introducing the ballot in the ballot box, would make it impossible for the ballot to be read by the system, which means that it will have to be counted manually at a stage posterior to the general ballot count. If such an attack were carried out on a large scale, it would distort the outcome of the provisional vote count.

5. Public presentations

Here are some public presentations that detail the analyzes carried out, the vulnerabilities found in the system and the possible attacks.

- «Vot.Ar: una mala elección» (“Vot.Ar: a bad election”). Iván Barrera Oro and Javier Smaldone. Ekoparty Computer Security Conference, Buenos Aires, Argentina. October 22, 2015. https://www.youtube.com/watch?v=WcgslNiP3AQ

- Demonstration of the ‘digital pointer’. Javier Smaldone, Plenary of Commissions of the Argentine Chamber of Deputies. August 4, 2016. https://www.youtube.com/watch?v=XA3JZ2HWQuA

- «Una mala elección (actualizada)» (“A bad election (updated)”). Iván Barrera Oro and Javier Smaldone, Ekoparty Computer Security Conference, Buenos Aires, Argentina. October 28, 2016. https://www.youtube.com/watch?v=q3PVNIVUd28

- «Remote detection of RFID recording». Alfredo Ortega and Javier Smaldone, Plenary of Commissions of the Argentine Senate. November 17, 2016. https://www.youtube.com/watch?v=Ay-r55E24zo

References

[1] «Real-world Electronic Voting: Design, Analysis and Deployment». Feng Hao and Peter Y. A. Ryan (editors). ISBN 978-1-49-871469-3. Auerbach Publications, 2016. Chapter 7: “Practical Attacks on Real-world E-voting”, J. Alex Halderman. https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf

[2] «El sistema de voto electrónico de la Ciudad de Buenos Aires: una “solución” en busca de problemas» (“The electronic voting system of the City of Buenos Aires: a ‘solution’ in search of problems”). Enrique Chaparro, 2015. https://archive.org/download/voto-electronico-CABA

[3] «Vot.Ar: una mala elección» (“Vot.Ar: a bad election”). Francisco Amato, Iván A. Barrera Oro, Enrique Chaparro, Sergio Demian Lerner, Alfredo Ortega, Juliano Rizzo, Fernando Russ, Javier Smaldone, Nicolas Waisman. 2015. https://archive.org/details/informe-vot.ar

[4] «Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales» (“Electronic voting. Between votes and machines. New technologies in electoral processes”). CIPPEC, María Inés Tula (coordinator). ISBN 950-9122-90-4. Editorial Planeta, 2005.