VOTO ELECTRÓNICO EN PARAGUAY

Boleta Única Electrónica: algunos riesgos y cómo mitigarlos

Javier Smaldone

TEDIC
TECNOLOGÍA & COMUNIDAD

VOTO ELECTRÓNICO EN PARAGUAY

Boleta única electrónica: algunos riesgos y cómo mitigarlos

Javier Smaldone

Un *white paper* es un informe o guía que informa de manera concisa y extensa sobre un tema complejo y presenta la filosofía y marco teórico al respecto.

Este *white paper* fue realizado por TEDIC en el marco de un proyecto financiado por el National Endowment for Democracy (NED) y forma parte de una serie de publicaciones que busca guiar e informar sobre el voto electrónico desde un enfoque político, legal, filosófico, técnico, social y cultural.

TECNOLOGÍA & COMUNIDAD

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

Coordinación: Maricarmen Sequera

Diseño de portada: Betania Ruttia

Diagramación: Horacio Oteiza

Corrección: Luis Pablo Alonzo Fulchi

DICIEMBRE 2020

Tabla de contenidos

1. Consideraciones generales

El presente trabajo tiene como base el sistema de voto electrónico *Vot.Ar* de la empresa *Grupo MSA* conocido como «boleta única electrónica». La principal referencia es su utilización en la República Argentina en las elecciones de 2015 en la Ciudad Autónoma de Buenos Aires (experiencia también analizada en [1]), 2016 en la Provincia de Mendoza, 2017 en la Provincia de Corrientes y 2017 en la Provincia de Salta.

La empresa propietaria del sistema, a pesar de múltiples requerimientos de ONGs y comunidades de profesionales informáticos, nunca ha permitido la inspección pública y abierta de su sistema, ni publicado siquiera partes del código fuente del *software*.

El acceso a los equipos ha sido posible solo en lugares de capacitación de partidos políticos o en lugares dispuestos para la demostración del sistema, no habiéndose podido nunca realizar una verdadera auditoría de los mismos.

Con respecto al *software*, en varias oportunidades se ha filtrado la porción que se distribuye en el DVD de inicio del sistema, que incluye los módulos de votación y escrutinio, y en una oportunidad el de transmisión de resultados.[1,2]

Las auditorías publicadas en los distritos donde se ha votado usando este sistema tampoco han brindado ningún detalle técnico relevante, omitiendo incluso la mención a ciertos componentes del sistema, que se han encontrado presentes en sistemas en uso en elecciones reales.[3]

Nunca se ha publicado ningún tipo de especificación técnica ni del *hardware* de la máquina de votación, escrutinio y transmisión, ni de los chips RFID utilizados en las boletas, actas y credenciales.

No se dispone de ningún tipo de información del *software* utilizado en los servidores para recibir los datos de las mesas transmitidos desde los centros de votación.

Por estas razones, el sistema actual puede diferir respecto del descripto en este artículo, ya sea por la existencia de elementos no detectados en las observaciones realizadas o por la cambios realizados por la empresa en el *hardware* o el *software* a través del tiempo.

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. Descripción del sistema

2.1. Hardware

La máquina de votación está compuesta por dos subsistemas: uno, al que llamaremos principal, basado en un procesador *Intel* y otro, al que llamaremos secundario, basado en un procesador *ARM* (ver figura 1).

El subsistema principal consta de una pantalla táctil del tipo resistiva, un lector de DVD (utilizado para la carga del sistema operativo y de las aplicaciones de votación y escrutinio, y de transmisión de resultados), conectores externos USB, Ethernet (red), VGA (vídeo) y de salida de audio analógico. Internamente posee una CPU *Intel Celeron* o *Atom* (dependiendo del modelo del equipo) y 2 gigabytes de memoria.

El subsistema secundario consta de una impresora térmica y un lector/grabador RFID (según norma ISO-15693). Ambos dispositivos están conectados a un microcontrolador ARM *Atmel* modelo AT91SAM7X256, que a su vez se conecta con el subsistema principal mediante un puerto USB. Dicho microcontrolador es accesible directamente mediante un conector JTAG.

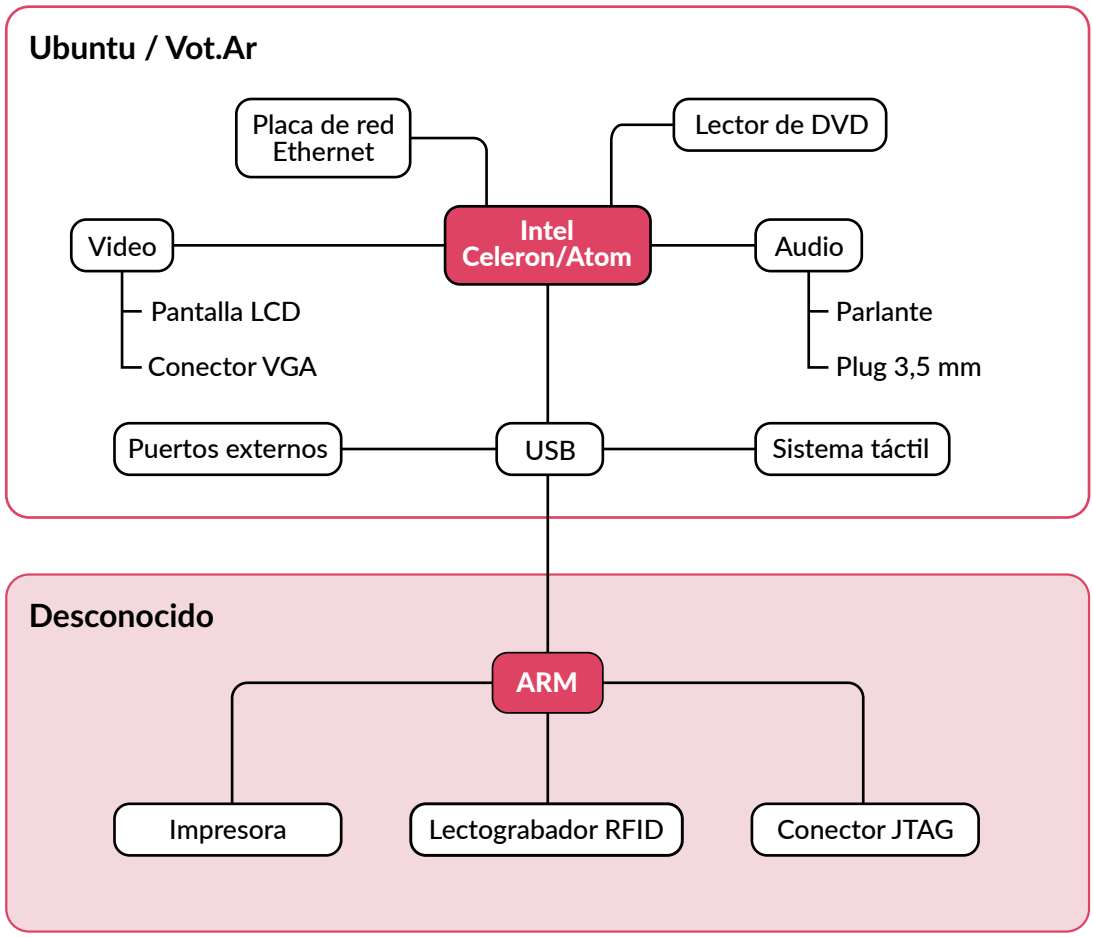


FIGURA 1: Arquitectura del sistema

La empresa nunca ha provisto un listado de materiales detallando los componentes físicos utilizados en los equipos y sus especificaciones. Para mayor detalle sobre el hardware utilizado, véase el informe [2], basado en los equipos utilizados en la Ciudad de Buenos Aires, Argentina, en julio de 2015.

FIGURA 2: Vista externa de la máquina de votación.

FIGURA 3: Vista inferior (baterías y cargador)

FIGURA 4: Panel superior (puertos)

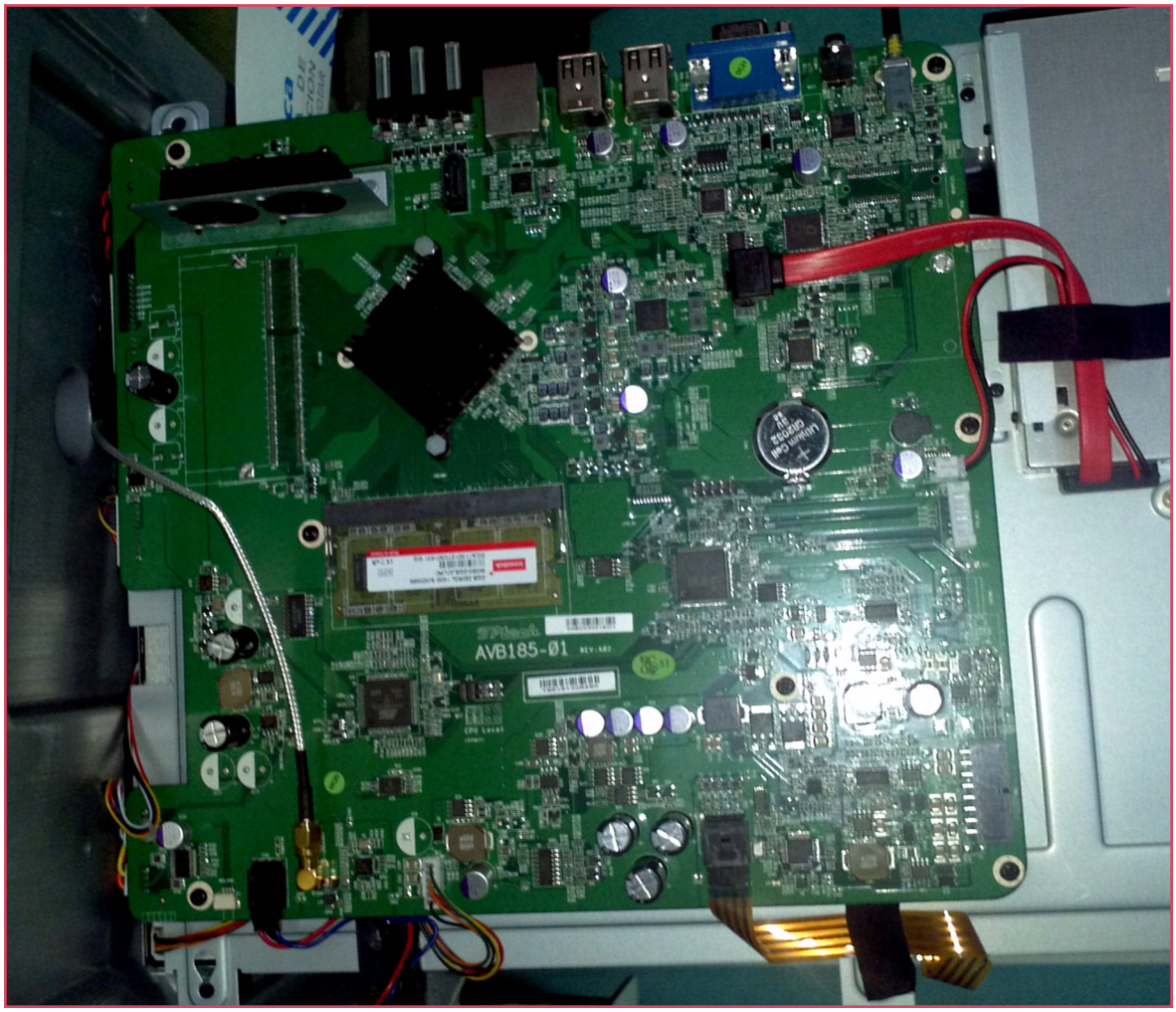


FIGURA 5: Placa base

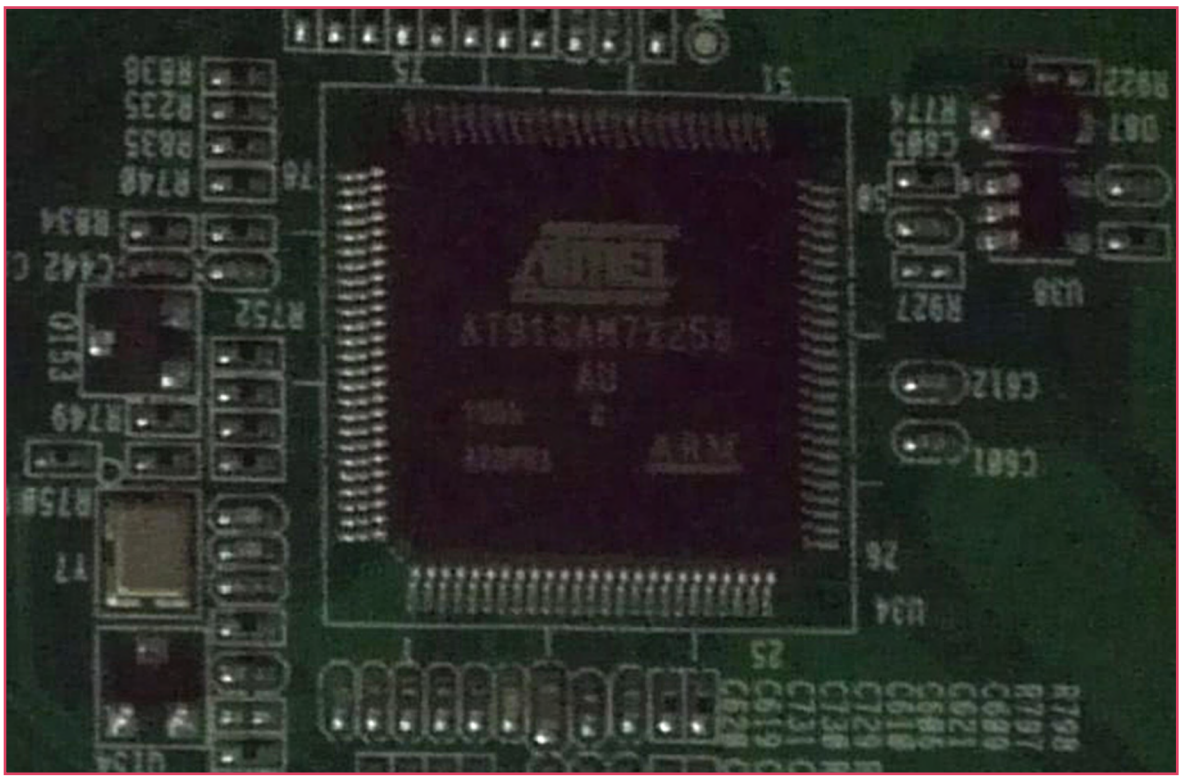


FIGURA 6: Microcontrolador AT91SAM7X256 (nunca auditado)

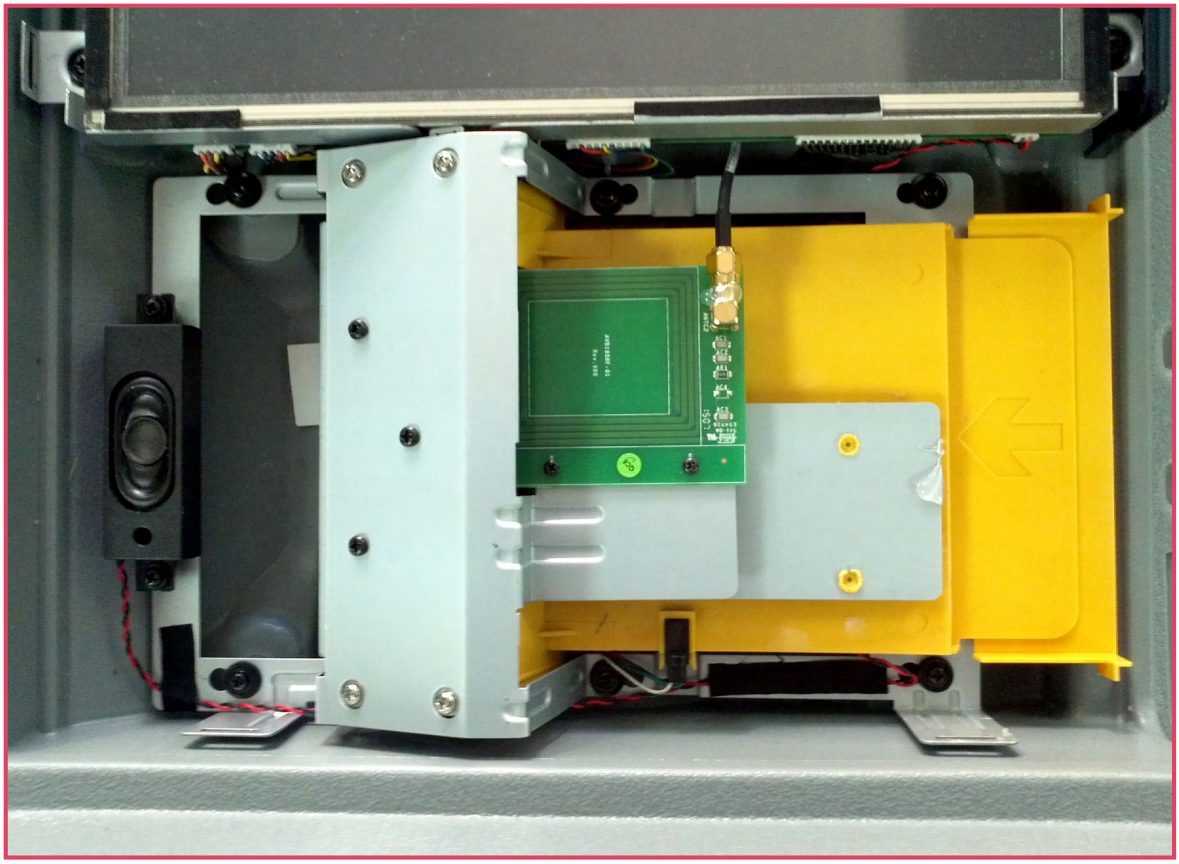


FIGURA 7: Impresora térmica y lector/grabador RFID

2.2. Software

2.2.1. Software de votación y escrutinio

El DVD que se entrega al presidente de mesa en sobre cerrado contiene una versión del sistema operativo *Ubuntu Linux* y el *software* de aplicación con las funcionalidades requeridas para la apertura de mesa, la votación, el cierre de mesa y el escrutinio de mesa. En el caso del sistema operativo y las librerías utilizadas, se trata de versiones estándares («off-the-shelf»), sin ningún tipo de personalización para su uso específico en un sistema de votación.

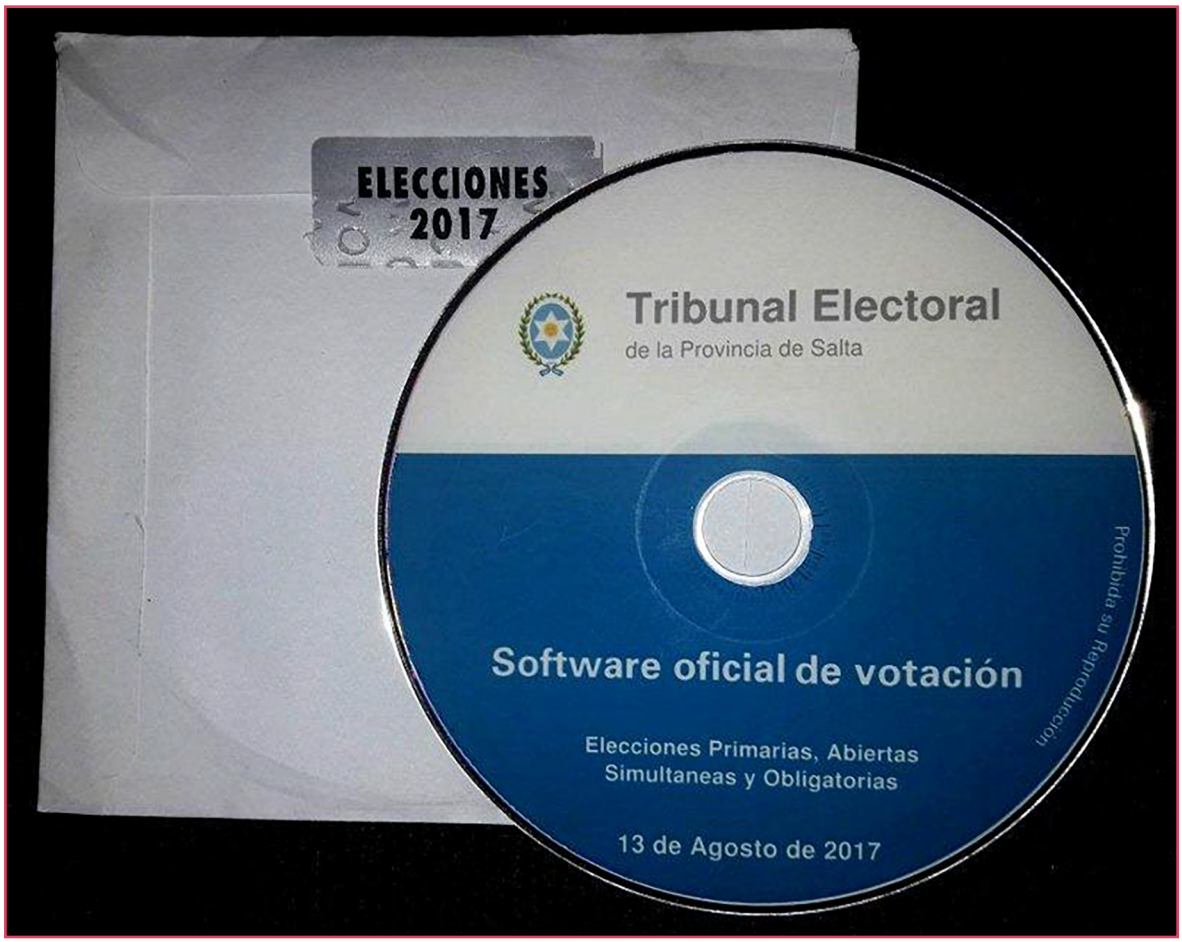


FIGURA 8: Software usado en elecciones de la Provincia de Salta, Argentina

2.2.2. Software de transmisión de resultados

El *software* de transmisión de resultados está contenido en un DVD usualmente en poder del personal técnico de la empresa proveedora, que también incluye una versión del sistema operativo *Ubuntu Linux*.

2.2.3. Software del microcontrolador Atmel

El *software* que se ejecuta en el microcontrolador Atmel, desarrollado en todo o en parte por la empresa *Grupo MSA*, es desconocido. Es el encargado de las siguientes funciones:

1. Recibir del subsistema principal los datos a imprimir en la boleta de papel, aplicarles el formato correspondiente y enviarlos a la impresora térmica.
2. Recibir del subsistema principal los datos a almacenar en el chip y enviarlos al lector/grabador RFID.
3. Recibir los datos leídos desde un chip por el lector/grabador RFID y enviarlos al subsistema principal.

2.2.4. Software de recepción de resultados

El *software*, alojado en los servidores de la empresa, que recibe los resultados enviados por el *software* de transmisión de resultados desde cada centro de votación nunca ha sido auditado ni pudo ser accedido públicamente. Como antecedente, en las elecciones de la Ciudad de Buenos Aires, Argentina, de julio de 2015, un investigador independiente detectó y denunció una grave vulnerabilidad que pudo poner en riesgo el escrutinio4. Dicho profesional fue denunciado penalmente, allanado y finalmente sobreseído.[4]

2.3. Chips RFID

Los chips RFID utilizados en las boletas y credenciales que hemos podido analizar son marca *NXP* modelos *ICODE SLI SL2 ICS206*[5] e *ICODE SLIX SL2S20027*[6], que operan según la norma ISO/IEC 15693 (*vicinity cards*) en una frecuencia de 13,56 MHz, con un alcance (según la norma y según el fabricante) de 1,5 metros.

2.3.1. Características generales

Una característica distintiva de esta tecnología es que cada chip RFID tiene un número único denominado «UID», fijado por el fabricante e inmodificable. Sin embargo, existen en el mercado chips con UID programable[7], que podrían ser utilizados en diversos tipos de ataques.

Los chips ICODE SLI y SLIX no incluyen mecanismos de autenticación, autorización ni cifrado, por lo cual tanto su lectura como su escritura puede ser realizada mediante cualquier dispositivo RFID/NFC que soporte la norma ISO 15693, más allá de las computadoras de votación utilizadas en el sistema, sin requerir ningún tipo de clave.

4 https://www.lanacion.com.ar/tecnologia/sobreseyeron-al-programador-que-revelo-fallas-en-el-sistema-de-boleta-unica-electronica-nid1924088/
5 https://www.nxp.com/docs/en/data-sheet/058031.pdf
6 https://www.nxp.com/docs/en/data-sheet/SL2S2002_SL2S2102.pdf
7 https://lab401.com/products/icode-sli-slix-compatible-uid-modifiable

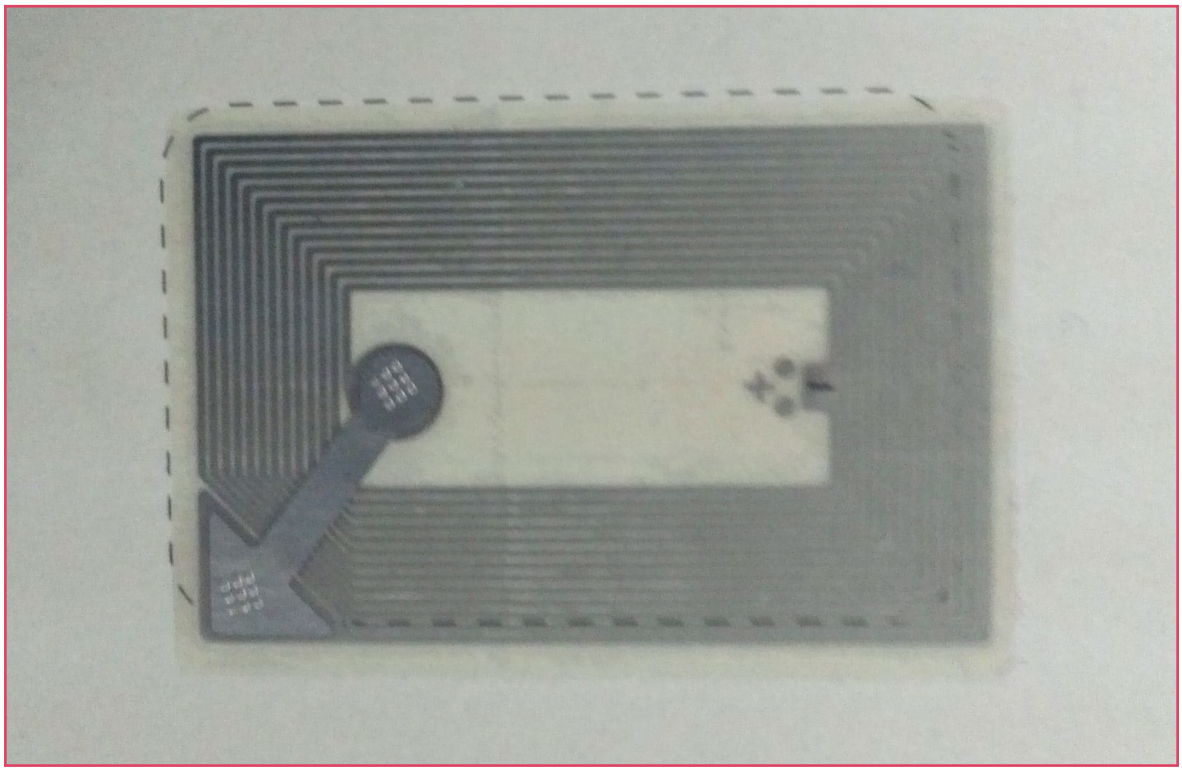


FIGURA 9: Chip RFID embebido en una boleta

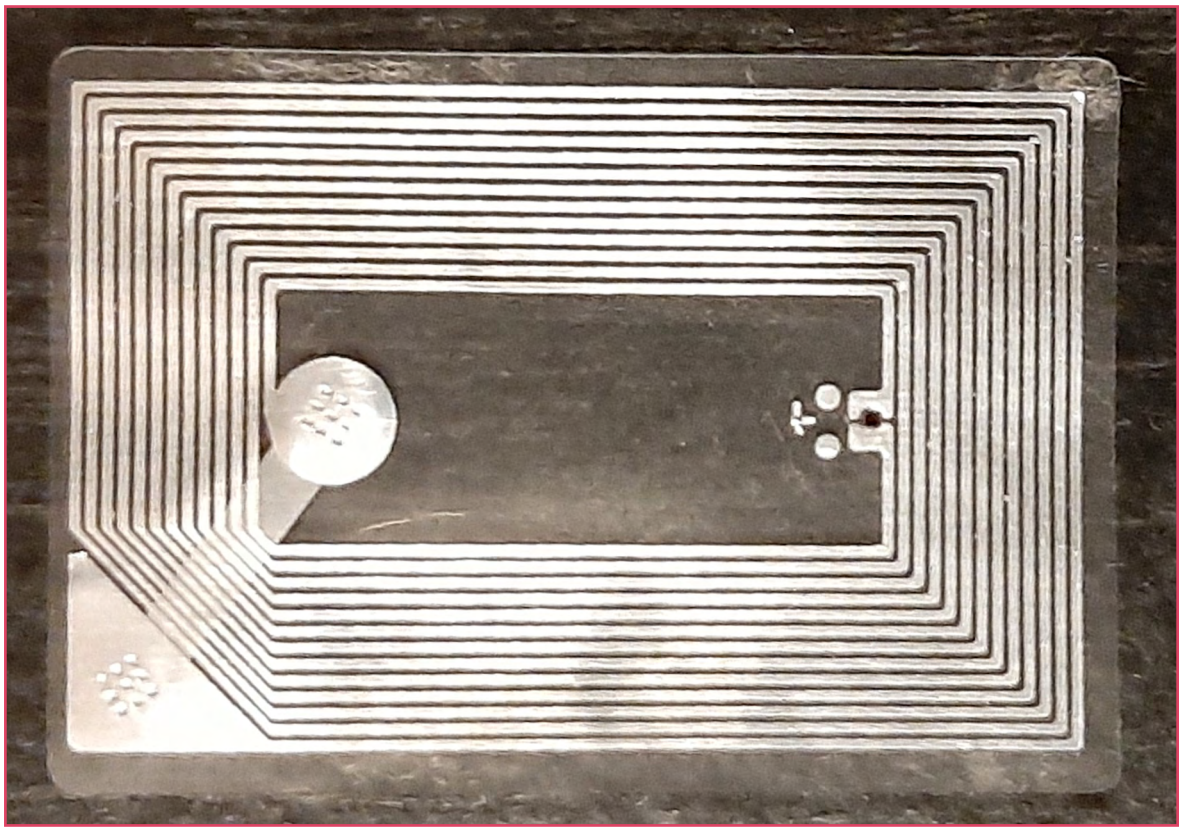


FIGURA 10: Chip RFID

2.3.2. Credenciales

Cada técnico de la empresa propietaria, como así también cada presidente de mesa, cuenta con una credencial para autenticarse ante el sistema, requisito para poder acceder a la funcionalidad reservada a cada tipo de usuario. Cada credencial cuenta con un chip RFID con un valor especial almacenado en un registro del mismo (que indica el tipo, diferenciándolas entre sí y también del resto de las boletas). Para mayor detalle, ver «B. 1. Estructura de datos» en [3].

2.3.3. Actas de mesa

Las actas de apertura, cierre y totales de mesa son generadas utilizando boletas con un color y texto distintivos que también contienen un chip RFID.

2.3.4. Votos

Cada boleta de voto incorpora un chip RFID del tipo ya descripto, generalmente con todos sus registros en cero (0), excepto el último que puede contener el valor «W_OK». En ninguna votación realizada en la Argentina con este sistema se ha usado ningún mecanismo de cifrado, por lo que la información de los votos es almacenada en los chips en forma de «texto plano», legible, reproducible y modificable por cualquiera que cuente con un dispositivo adecuado.

FIGURA 11: Boleta de voto (anverso y reverso)

3. Principios de uso

3.1. Apertura de mesa

Una vez dispuesta la máquina de votación en el lugar elegido y conectada a la alimentación eléctrica, se procede a introducir el DVD con el *software* de votación y escrutinio. Al encenderla, y luego de las pantallas de inicio del BIOS, comenzará la carga del sistema operativo y finalmente de la aplicación de votación.

Una vez iniciado el sistema, el presidente de mesa debe proceder a la apertura de la votación. Para eso, selecciona la opción «Apertura de Mesa» y acerca al lector RFID su tarjeta de identificación e introduce una clave (PIN), ambos elementos entregados en sobre cerrado junto con el material de la mesa.

Luego debe proceder a emitir el acta de apertura. Para ello se introducirá una boleta especial en la que se imprimirán y grabarán los nombres de las autoridades de mesa y fiscales. La misma será utilizada al finalizar la votación para realizar el cierre de la mesa, como así también en caso de tener que reiniciar la máquina de votación o reemplazarla por otra.

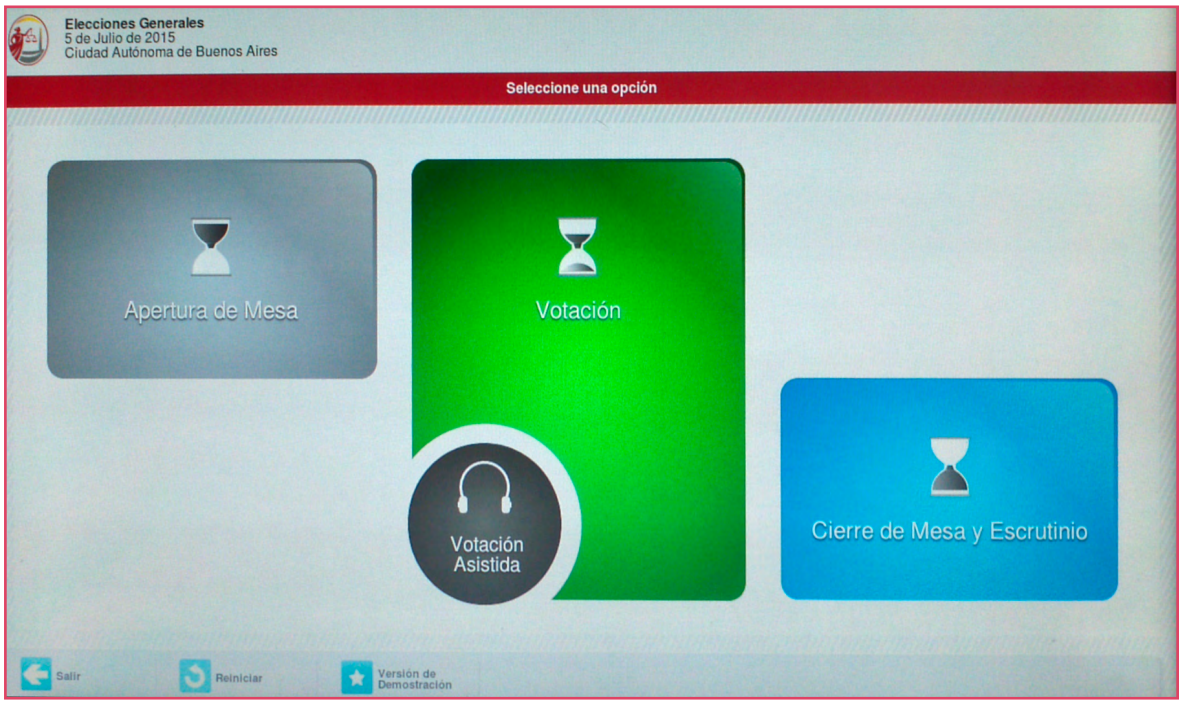


FIGURA 12: Pantalla principal del sistema de votación y escrutinio

3.2. Votación

Una vez identificado el votante, el presidente procede a entregarle una boleta electrónica cuyo papel está en blanco. Antes de hacerlo, retiene para sí la mitad superior del troquel de la boleta.

El votante se dirige a la máquina de votación, introduce la boleta en la ranura a tal efecto y el sistema procede a mostrarle la oferta electoral. Ante alguna anomalía en el chip la máquina expulsa la boleta, debiendo en tal caso el votante reclamar una nueva.

Luego de realizar la composición de su voto, el votante debe confirmar la misma. Inmediatamente después, el lector/grabador RFID graba los datos en el chip y la impresora tracciona la boleta, imprime el voto en el papel y la expulsa.

Una vez hecho esto, el votante puede acercar el chip RFID al lector, y en tal caso la máquina procederá a su lectura y mostrará en la pantalla los datos obtenidos.

Luego el votante debe plegar la boleta al medio, haciendo coincidir la chapa metálica en un extremo con el chip RFID en el otro, y regresa a la mesa. El presidente de mesa desprenderá la mitad inferior del troquel de la boleta y verificará la coincidencia con la mitad superior en su poder.

Finalmente, la boleta es depositada por el votante dentro de la urna.

3.3. Cierre de mesa

Al finalizar la votación, el presidente de mesa aproxima su credencial al lector RFID, introduce su PIN y luego elige la opción de «Cierre de Mesa y Escrutinio». Debe introducir la boleta especial y en ella se imprimirá y grabará el horario de cierre de la votación.

3.4. Escrutinio

Para dar comienzo al conteo de los votos, se debe aproximar al lector/grabador RFID el acta de cierre de la mesa, pasando el *software* a «modo de escrutinio». Luego, se procede a la lectura de los chips RFID de cada una de las boletas de votación, y la máquina contabiliza los datos leídos mostrando además en la pantalla el detalle de cada boleta.

Al finalizar, se emite una boleta especial denominada «acta de resultados de mesa», conteniendo los totales impresos en el papel y grabados en el chip RFID de la misma. Al menos en el sistema analizado, no se prevé ninguna instancia de corrección manual de los resultados.

3.5. Transmisión de resultados

Para realizar la transmisión de resultados de las mesas, un empleado de la empresa toma una máquina de votación y la inicia con un DVD especial que contiene el *software* utilizado a tal efecto. Una vez conectada la máquina a Internet (usando conexión de red ethernet, un módem 4G o alguna otra tecnología de conectividad disponible), procede a leer los chips RFID de cada una de las actas de mesa y, previa visualización de los datos leídos que deberían ser verificados por las autoridades electorales presentes, procede a su envío hacia un servidor central de la empresa.

4. Ataques

A continuación se describen algunos ataques que se han determinado posibles (y en muchos casos ensayados a nivel de «prueba de concepto») sobre el sistema *Vot.Ar*. Para este análisis se han considerado como posibles atacantes a los siguientes actores:

- Votantes.
- Autoridades de mesa.
- Fiscales partidarios.
- Empleados de la empresa proveedora.
- Técnicos contratados para los comicios.
- Proveedores de la empresa proveedora (y por transitividad, proveedores de aquellos).

4.1. Suplantación de credenciales

4.1.1. Credencial de técnico

La credencial de técnico permite el acceso a opciones de configuración del sistema. Entre ellas se encuentran, por ejemplo, la calidad de la impresión y la posibilidad de expulsar el DVD. Para generar una credencial de técnico basta con un chip RFID con el valor 0x0002 almacenado en los bytes 2 y 3.

Mitigación: No hay forma de mitigar este ataque sin un rediseño del sistema de autenticación.

4.1.2. Credencial de presidente de mesa y acta de apertura

La credencial de presidente de mesa permite la emisión de las actas de apertura y cierre, como así también la habilitación del modo de votación. La misma debe ir acompañada del PIN, que también se entrega en sobre cerrado y sellado. Dicha credencial puede generarse utilizando un chip RFID con el valor 0x0003 almacenado en los bytes 2 y 3.

Todas las funciones del presidente de mesa pueden ser realizadas sin contar con la credencial y el PIN correspondientes, teniendo un acta de apertura válida. Para generar un acta de apertura, basta con grabar en un chip RFID el valor 0x0005 en los bytes 2 y 3. Al acercar al lector RFID un acta de apertura, no se solicita ni la credencial ni el PIN del presidente de mesa.

Mitigación: No hay forma de mitigar este ataque sin un rediseño del sistema de autenticación.

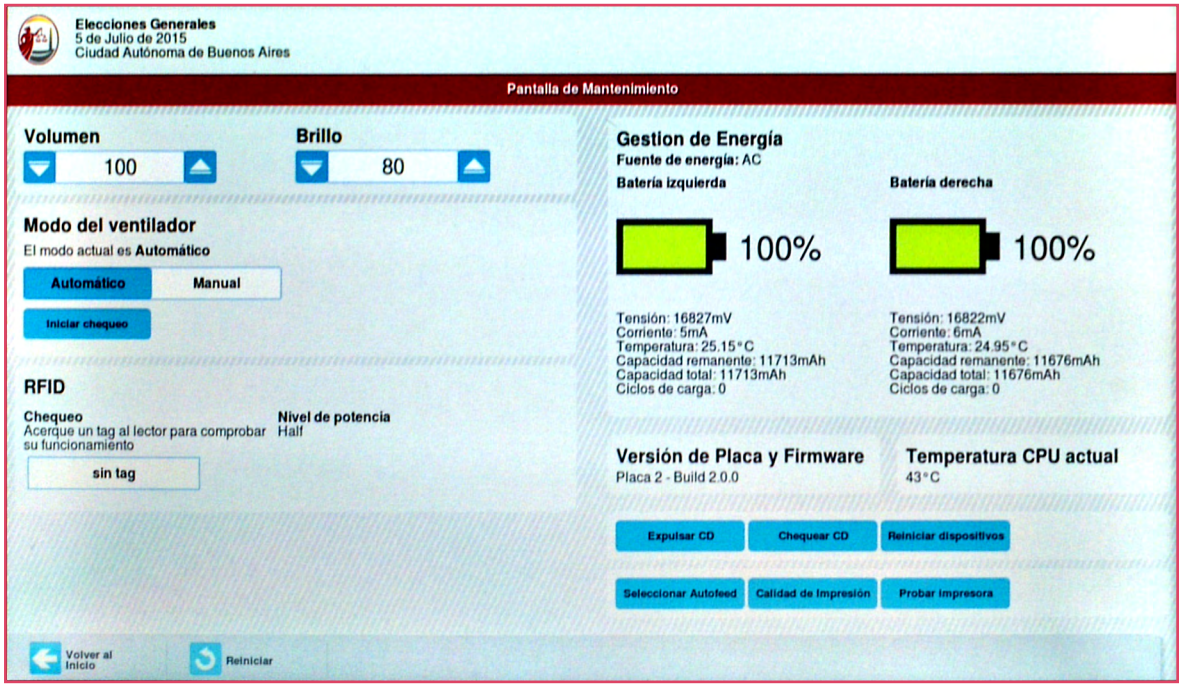


FIGURA 13: Modo de mantenimiento (accesible mediante una credencial del técnico)

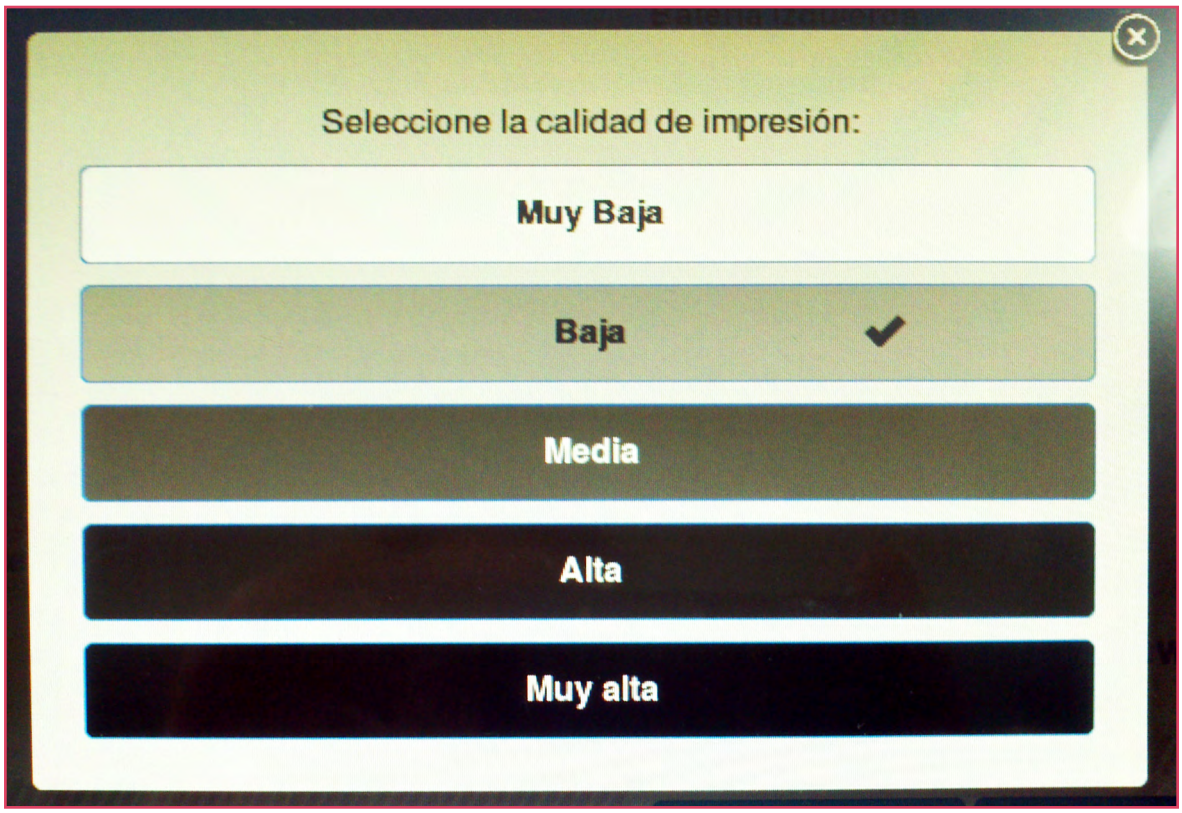


FIGURA 14: Selección de la calidad de impresión

4.2. Duplicación de actas

Tanto las actas de apertura como de cierre pueden ser generadas escribiendo valores determinados en un chip RFID, ya que el sistema no utiliza, al menos en las versiones analizadas, ninguna función de cifrado o mecanismo que permita verificar la autenticidad de las mismas. Para ello puede usarse una boleta común de votación, ya que todas utilizan el mismo tipo de chip.

Mitigación: No hay forma de mitigar este ataque sin un rediseño del sistema de generación de actas.

4.3. Identificación de los chips

Como se dijo, cada chip RFID posee un identificador único (UID). Esto resulta en que cada boleta de votación se encuentra numerada de una forma no visible al ojo humano, pero sí detectable por distintos dispositivos. Si se pudiera determinar qué UID corresponde al chip de la boleta entregada a determinado votante, podría luego determinarse cómo votó, rompiendo el secreto.

Mitigación: Una forma de mitigar parcialmente este ataque es permitir que el votante elija una boleta arbitraria, cuidando que no haya en las cercanías de la mesa ningún dispositivo capaz de leer el UID del chip RFID de la misma.

4.4. Quema de chips

Los chips RFID son pasivos, esto es, no tienen energía propia provista por una batería. Obtienen la energía eléctrica necesaria para su funcionamiento de la misma señal de radio que recibe del lector/grabador. Si se genera una señal demasiado potente, el chip puede sobrecargarse y quemarse. En experiencias realizadas con dispositivos generadores de pulsos electromagnéticos de baja intensidad (ver figura 15), se ha logrado quemar los chips RFID utilizados en este sistema desde un par de centímetros[8]. Utilizando mayor potencia, puede llegar a realizarse el mismo ataque desde una distancia suficiente como para quemar todos los chips de las boletas depositadas en una urna, impidiendo su conteo automatizado, o todos los chips de las boletas en poder del presidente de mesa, impidiendo en este caso la votación.

Mitigación: Para mitigar este ataque pueden depositarse las boletas en blanco en algún recipiente que genere un efecto «jaula de Faraday», y dotar a la urna de una protección del mismo tipo.

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

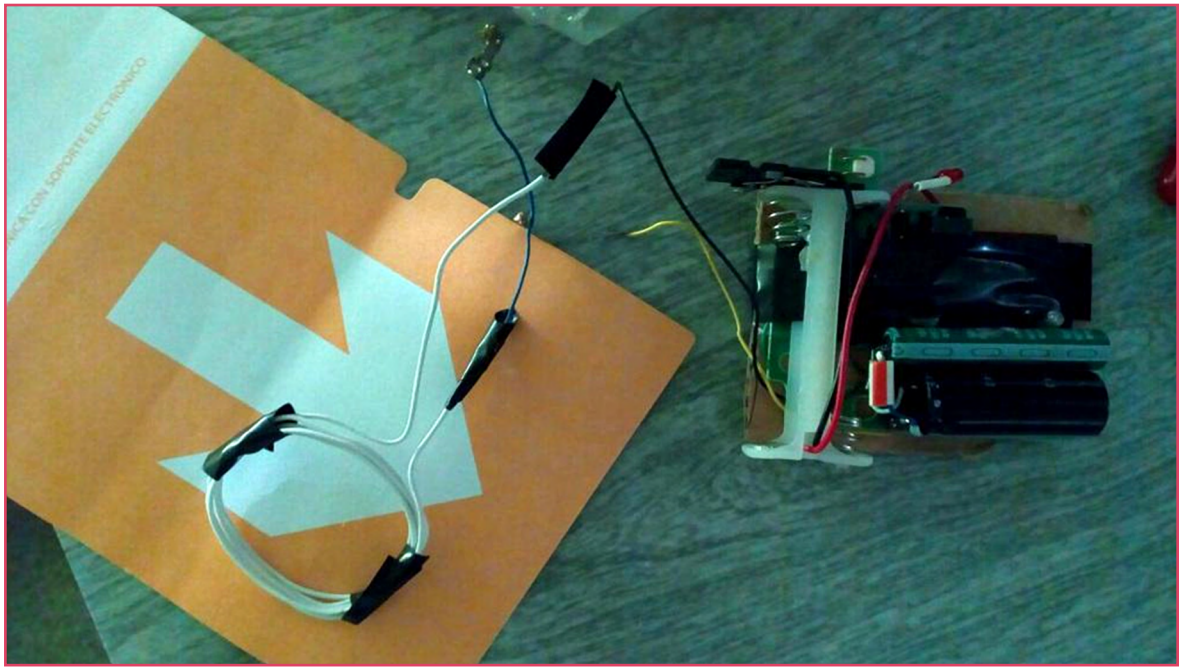


FIGURA 15: Quemador de chips RFID

4.5. Manipulación de software

El sistema *Vot.Ar* ha incorporado en las últimas versiones analizadas funciones de verificación en el arranque del sistema (*secure boot*) pero aún existen formas de alterar el *software*, ya sea en el DVD utilizado para distribuirlo a cada mesa de votación, como también probablemente en tiempo de ejecución una vez iniciado el sistema. Además, debido a que el *hardware* utilizado no posee un «secure element», el mecanismo de «secure boot» puede ser manipulado por alguien con acceso físico a las máquinas. Por otra parte, el *software* que se ejecuta en el microcontrolador Atmel encargado de las tareas de impresión y lectura/grabación de los chips RFID puede ser modificado accediendo a la interfaz JTAG dispuesta a tal efecto.

Es posible realizar cambios maliciosos en el *software* que resulten indetectables en pruebas de «caja negra», es decir, que no puedan ser descubiertas haciendo pruebas de uso. Esto puede lograrse permitiendo que el sistema funcione de forma lícita salvo que se produzca algún evento externo a modo de señal (como por ejemplo, la lectura de un chip RFID con ciertos valores, o una serie de clics sobre ciertas áreas de la pantalla) que habilite el comportamiento malicioso.

Además, como se utiliza una distribución de *software* estándar, sin una personalización específica (*Ubuntu Linux*) existe gran cantidad de componentes de *software* que no están bajo control de la empresa proveedora del sistema. Por lo tanto, ante la eventual detección y publicación de problemas de seguridad en alguno de ellos, por ejemplo en los días previos a la elección, no será posible su actualización.

4.5.1. Emisión

Manipulando el *software* de emisión pueden implementarse varias formas de fraude. La más simple es dificultar la elección de un candidato o partido, por ejemplo haciendo que tienda a aparecer en lugares menos destacados de la pantalla o simulando errores de selección atribuibles a las limitaciones de la pantalla táctil.

En la presentación realizada por el autor en el Senado de la Nación Argentina se mostró como ejemplo un ataque sobre el *software* del microcontrolador Atmel[9] que permite reemplazar la selección del votante por otra arbitraria, de forma que pueda pasar inadvertida por parte del mismo o, en caso de ser detectada, atribuida a un error del votante o descartada como una falsa denuncia.

También puede darse el caso de un elector declamando que emitió un voto por un candidato resultando en un voto impreso en favor de otro, y adjudicando la situación a una falla (intencionada o no) del sistema. La veracidad de dicha afirmación sería incomprobable, pero generaría como mínimo una demora para el resto de los votantes (y, de realizarse de forma generalizada en muchas mesas, posiblemente algún tipo de tumulto).[10]

El hecho de que el sistema tenga dos registros del voto emitido, uno impreso en el papel y otro grabado en el chip posibilita que el *software* pueda ser modificado para que ambos no coincidan, y que alguno de ellos o ambos tampoco coincidan con la intención del votante. Esto permitiría una variedad de ataques que facilitarían la comisión de fraude en diversas formas. Además, la verificación del voto almacenado en el chip RFID para contrastarlo con lo impreso en el papel se realiza mediante la misma computadora con la que fue emitido, volviéndola completamente inútil.

Mitigación: Para reducir el riesgo de este tipo de ataques, deberían verificarse los DVD utilizados en cada máquina de votación, calculando los «hash» correspondientes para verificar que coincidan con los registrados previamente por la autoridad electoral. Debería verificarse también la integridad del código almacenado en el microcontrolador Atmel, exigiendo se retire el cable que permite acceder externamente al puerto JTAG (ver figura 16). En ambos casos, además, se hace indispensable la publicación del código fuente del *software* y el diseño detallado del *hardware*. Debería incorporarse además un segundo dispositivo, independiente de la máquina emisora del voto, para que el votante pudiera verificar los datos almacenados en el chip RFID. En el escrutinio, deberá prestarse especial atención a que el contenido leído desde cada chip RFID se corresponda con lo impreso en cada boleta de papel.

9 https://www.youtube.com/watch?v=rd1aOFXZl5Q

10 Ver lo ocurrido en las elecciones de la ciudad de San Luis, Argentina, en noviembre de 2017: https://www.lmneuquen.com/escandalo-fraude-san-luis-una-maquina-emitia-votos-el-partido-del-intendente-n570919

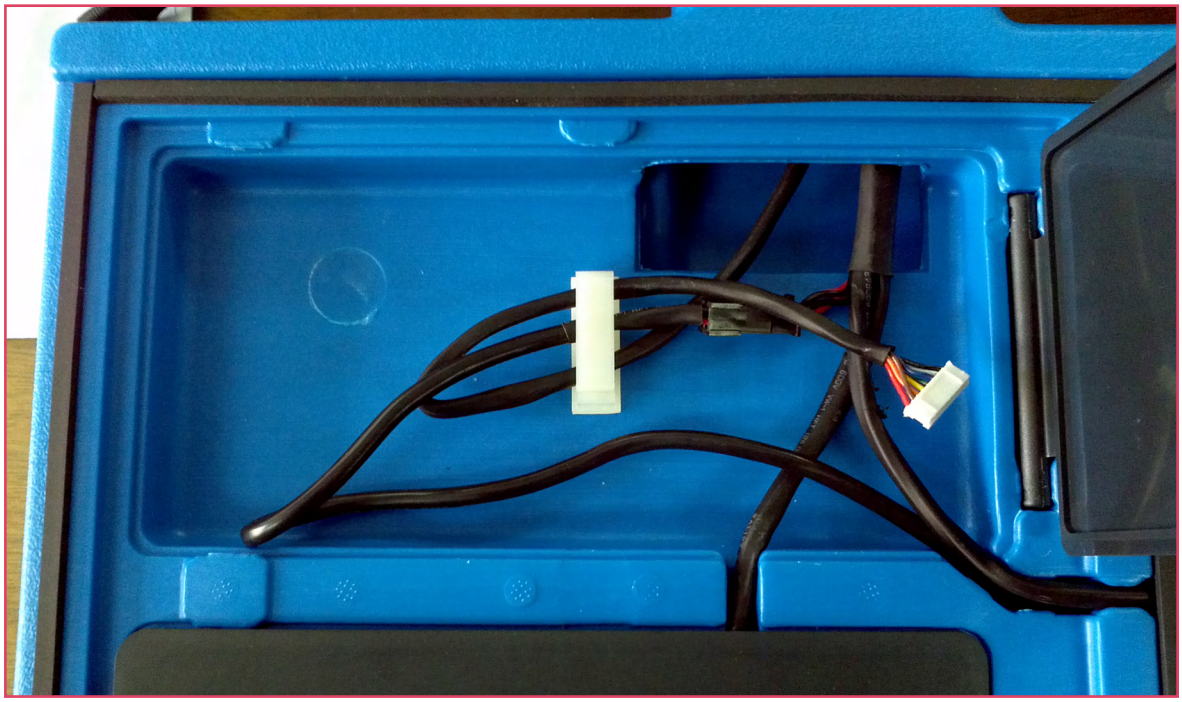


FIGURA 16: Cable JTAG en la base de la máquina

4.5.2. Escrutinio

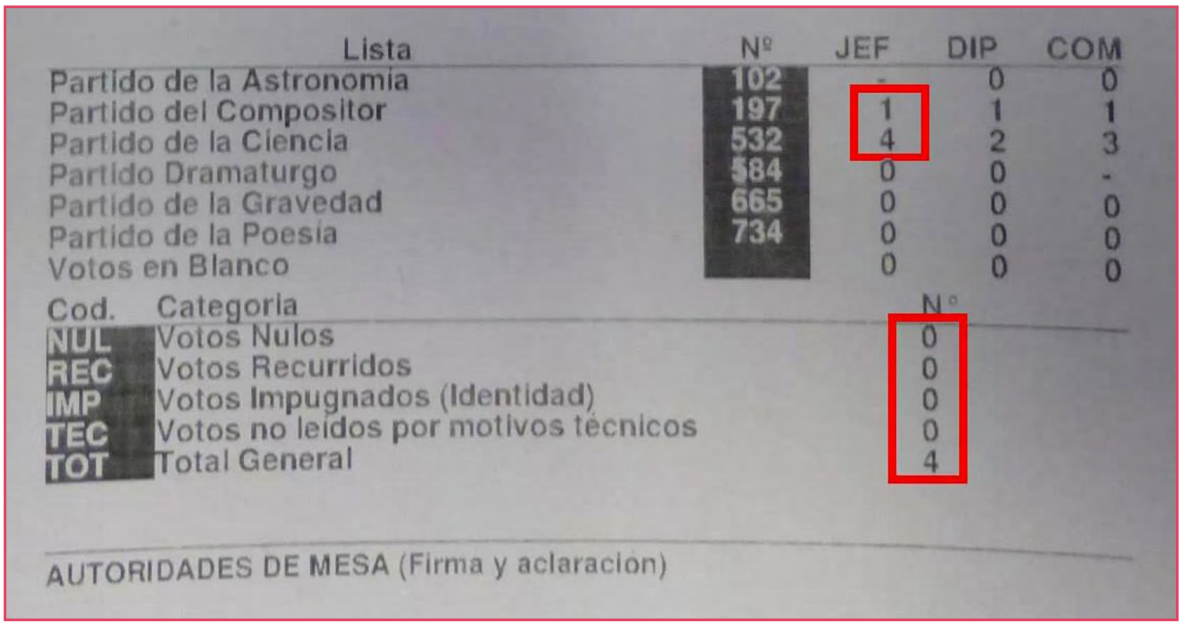
La modificación del *software* de escrutinio puede permitir alterar el conteo de los votos. En las experiencias de varias elecciones argentinas, se ha apreciado que los presidentes de mesa y fiscales partidarios tienden a confiar en el sistema informático y no realizan un escrutinio independiente para corroborar los resultados.

En el año 2015, investigadores independientes encontraron un error en el sistema de escrutinio que permitía que un chip RFID almacenara más de un voto, y el sistema los contabilizaba como lícitos. De no controlar el conteo, la situación podía pasar inadvertida, dando como resultado una cantidad de votos mayor a la real. Este ataque, denominado «multivoto» (ver figura 17) no había sido detectado por ninguna auditoría realizada hasta ese momento (al menos dos de la Universidad Nacional de Salta y una de la Universidad Nacional de Buenos Aires)[11]. No puede descartarse la existencia de otros errores o la introducción maliciosa de comportamientos similares si logra alterarse el *software* de escrutinio mediante alguna maniobra.

Mitigación: El presidente de mesa y los fiscales partidarios deben llevar un conteo independiente, comprobando que el contenido de cada chip RFID se corresponda con los datos impresos en el papel de la boleta y dejando registro escrito de cualquier discrepancia.

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

FIGURA 17: Ataque «multivoto»



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	N°
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)

FIGURA 18: Acta inconsistente procuto del «multivoto»

4.6. Rellenado de urnas

El acta de cierre del sistema no incluye ninguna información sobre la cantidad de votos emitidos durante la jornada. Esto se debe a que en medio de la misma el sistema puede ser reinicializado o incluso la máquina de votación puede ser reemplazada por otra. Durante el escrutinio el sistema contabiliza cada voto leído y al final informa, en el acta de resultados de mesa, la cantidad total de votos.

En la experiencia de varias elecciones argentinas, hemos observado que las autoridades de mesa no contrastan la cantidad de votos contabilizados por el sistema con la cantidad de votos emitidos, ya que el sistema no permite introducir este último dato y no existe ningún documento confeccionado manualmente.

Por otra parte, la boleta de votación no incorpora ninguna medida de seguridad para garantizar que corresponda a la mesa donde supuestamente fue emitida (más allá del troquel utilizado durante la emisión del voto, pero que es desprendido totalmente antes de que la boleta sea introducida en la urna).

Luego de emitir su voto usando el sistema, el votante regresa a la mesa de votación con la boleta doblada y sujeta entre sus manos. En ningún momento el votante se desprende de la misma, ni mucho menos la desdobla, por lo cual es imposible a simple vista determinar si se trata de una sola boleta o varias. De esta forma, un votante podría por ejemplo introducir dos boletas en la urna: una válidamente emitida en el acto y otra previamente impresa que le hubiera sido entregada con anterioridad.[12] En el momento del escrutinio resultaría imposible diferenciarlas y, si además no se contrastara la cantidad de boletas con la cantidad de votantes, la situación pasaría completamente inadvertida.

12 Un ejemplo de esta maniobra puede verse en https://www.youtube.com/watch?v=fBUe3fKMSFQ

Mitigación: Llevar un conteo de la cantidad de votantes que emitieron su voto. Realizar un acta manual que refleje dicha cifra. Dotar la boleta de alguna medida de seguridad física que permita determinar si es un voto válido o no (por ejemplo, la firma del presidente de mesa y los fiscales, un sello con el número de la mesa, etc.).

4.7. Agregado de votos falsos

Mediante la utilización de chips RFID con UID programable (hoy disponibles en el mercado) y un dispositivo lector/grabador podría alterarse el escrutinio, «inyectando» votos falsos en el sistema. También podría utilizarse a tal efecto un emulador de chips RFID, como un dispositivo Proxmark3[13], ChameleonMini[14] o similar, para realizar el añadido de votos.

Mitigación: Fiscalizar debidamente el escrutinio, para evitar que sean agregados votos falsos.

4.8. Lectura remota de chips

La tecnología RFID se basa en la transmisión de información mediante ondas de radio. Según las especificaciones del fabricante los chips utilizados en este sistema, su lectura es posible hasta desde una distancia de 1,5 metros (dependiendo del tamaño de la antena y la potencia).

4.8.1. Durante la emisión del voto

Debido a la naturaleza de las ondas de radio emitidas por el grabador RFID, e independientemente de las especificaciones técnicas del chip, las mismas son perceptibles desde una distancia bastante mayor a 1,5 metros. Esto ha sido demostrado en pruebas de laboratorio y expuesto públicamente en el Senado de la Nación Argentina.[15]

El ataque consiste en analizar las ondas de radio recibidas por un receptor en la frecuencia de 13,54 MHz (onda corta) y analizar el sonido. Utilizando un smartphone con NFC (de menor potencia que el lector/grabador RFID de las máquinas de votación) con una app de grabación[16], un receptor de radio hogareño conectado a una notebook y *software* de detección[17], se logró diferenciar dos patrones distintos de bits (datos) con una precisión del 100 % desde 2 metros de distancia y con más de un 80 % desde 2,70 metros. Esto podría permitir determinar si un candidato vota o no por determinado partido político.

Este tipo de ataques, conocidos como «side-channel», también podrían realizarse mediante el análisis de otras variables, tales como consumo eléctrico, nivel de ruido, emisión electromagnética de los componentes (radiación de Van Eck), etc. Estas técnicas han sido utilizadas para romper el secreto en sistemas de voto electrónico de los Países Bajos[18] y Brasil[19].

---

13 https://hackerwarehouse.com/product/proxmark3-rdv4-kit/
14 https://lab401.com/products/proxgrind-chameleon-mini-revg
15 https://www.youtube.com/watch?v=yrFSQBj1Emo
16 https://github.com/tristangrimaux/Nemo
17 https://github.com/ortegaalfredo/nfcread
18 https://www.youtube.com/watch?v=hwz1BLRgTg0
19 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/

Mitigación: Con el diseño actual del sistema, no existe forma de mitigar completamente este ataque. Para reducir el riesgo debe configurarse el lecto/grabador RFID de la máquina de votación en la potencia mínima (opción prevista en el código fuente del *software* de votación).

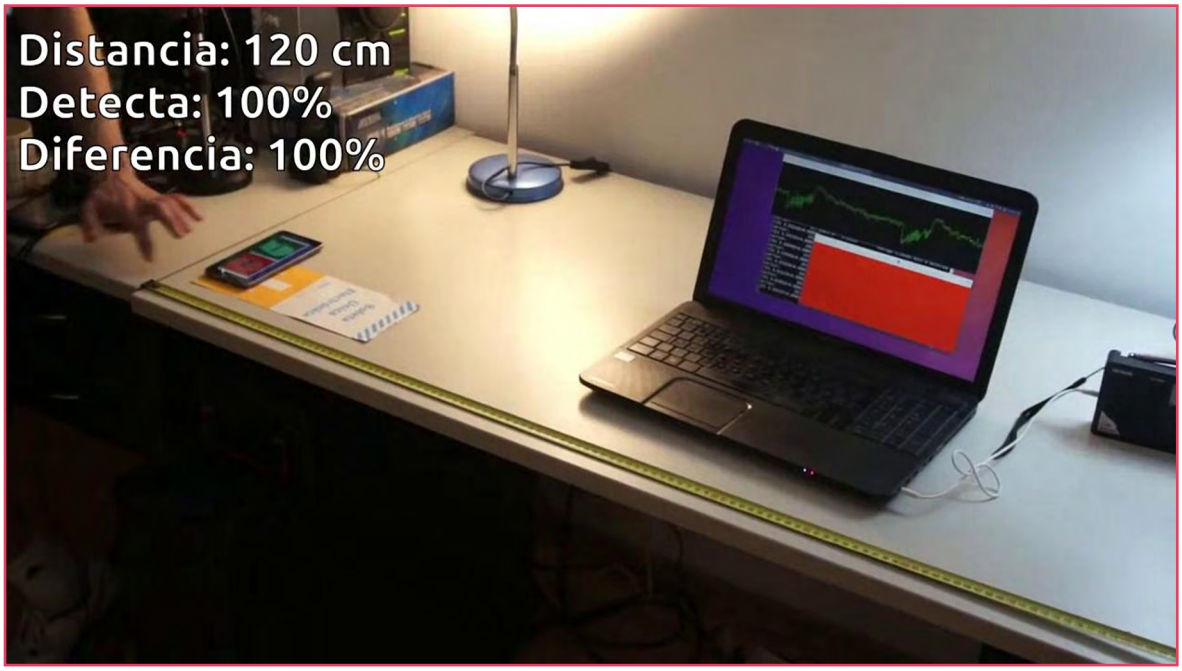


FIGURA 19: Diferenciación de escritura en chips RFID

4.8.2. Luego de la emisión del voto

Como se dijo en 2.3.4, los votos son grabados en los chips sin utilizar ningún mecanismo de cifrado. Por lo tanto, su contenido puede ser leído por cualquier lector RFID o NFC (como por ejemplo, el incluido en muchos modelos de smartphones). En el año 2015, se desarrolló una aplicación denominada «Puntero digital»[20], para ejemplificar cómo usando un smartphone, posiblemente oculto entre las ropas del votante, este podía demostrarle a un tercero la composición de su sufragio, posibilitando la compra de votos. Esta aplicación fue presentada también en la Cámara de Diputados de la Argentina en agosto de 2016[21]. El mismo ataque podría lograrse mediante un dispositivo fabricado a tal efecto, con un costo sensiblemente menor al de un smartphone y con menores dimensiones.

Mitigación: Habilitar las funciones de cifrado de los votos ya incluidas en la versión de 2017 del *software*.

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

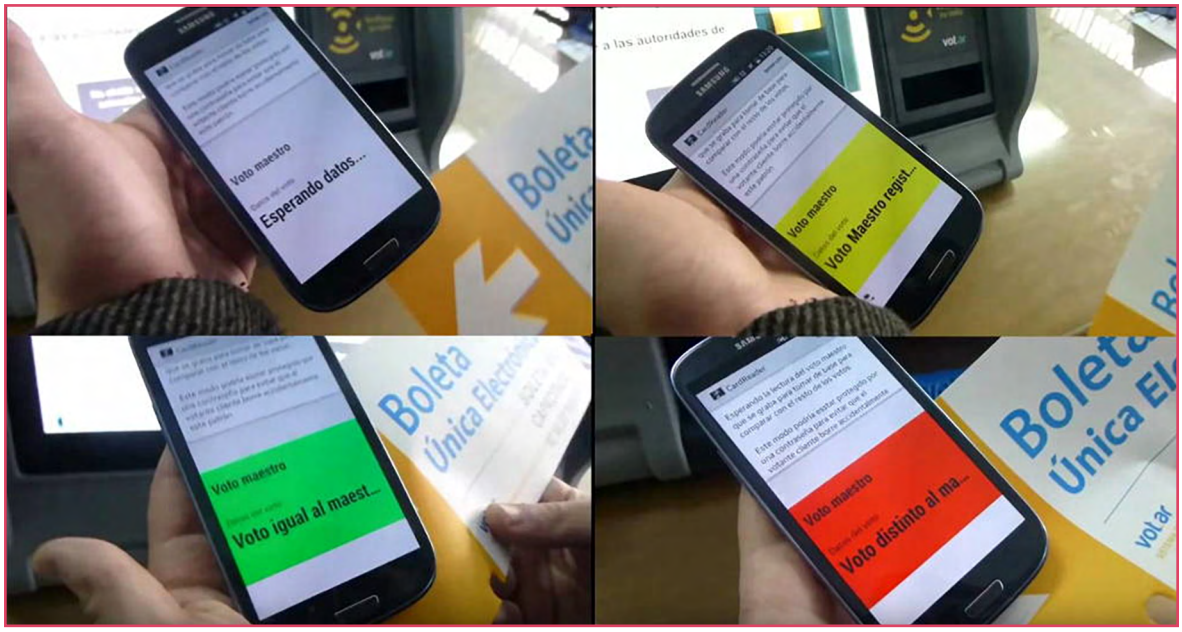


FIGURA 20: Aplicación «Puntero digital»

4.8.3. Dentro de la urna cerrada

Según [4], el sistema fue diseñado originalmente para que los votos pudieran ser escrutados de forma remota, sin necesidad de abrir la urna:

> «El escrutinio de mesa no requiere la apertura de la urna. Esto es posible dado que todas las BVE [Boletas de Voto Electrónico] cuentan con un chip propio (TAG RFiD) que puede ser leído por la interrogación de una simple antena de RF desde el exterior [...]. Según la empresa, este es uno de los nuevos elementos de seguridad incorporados, por los que solo el elector toca su voto. La apertura de la urna podría efectuarse ante un caso de extrema necesidad y solo por parte de la autoridad competente».

La propia patente obtenida en la Argentina por la empresa *Grupo MSA* en el año 2007[22] reconoce que:

> «Otro objeto del presente invento es proveer de medios para asegurar el secreto del voto en la boleta de voto electrónico, entre los que se encuentra la lectura de la totalidad de los TAG-RFID dentro de la Urna, sin necesidad de tener que abrirla, evitando todo contacto manual con los votos».

Mitigación: Si bien en versiones posteriores del sistema se agregó una lámina de metal en la boleta, que al plegarse coincide con el chip RFID y absorbería las ondas de radio imposibilitando su lectura, tal mecanismo solo funciona si la separación entre ambos elementos es mínima (menor a 4 o 5 milímetros). Una posible forma de mitigar este tipo de ataques sería agregar a los extremos de la boleta algún tipo de adhesivo que permita mantenerla plegada permanentemente. También podría dotarse a la urna de algún recubrimiento que genere un efecto de «jaula de Faraday».

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

4.9. Vandalismo

4.9.1. Máquinas de votación

Existen múltiples formas de afectar el normal funcionamiento de las máquinas de votación, desde daños producidos en la pantalla táctil con algún elemento cortante, hasta la inyección de líquido a través de algunos de los puertos que son fácilmente accesibles desde el exterior del chasis. También pueden realizarse ataques al sistema de alimentación eléctrica, limitando el funcionamiento de las máquinas solo al tiempo de autonomía provisto por las baterías. En elecciones argentinas se han visto ataques sobre la impresora térmica, introduciendo chicles o colillas de cigarrillo a fin de inutilizarlas.

4.9.2. Boletas y actas

Además del ataque por pulso electromagnético descripto en 4.4, también puede destruirse un chip físicamente, utilizando algún elemento punzo-cortante como un bolígrafo o una aguja. Esto, si se realiza después de emitir el voto y antes de introducir la boleta en la urna, imposibilitaría su lectura mediante el sistema, debiendo ser luego contabilizado de forma manual en una etapa posterior al escrutinio de mesa. Si un ataque de este tipo se llevara a cabo a gran escala, distorsionaría el resultado del escrutinio provisorio.

5. Presentaciones públicas

A continuación, algunas presentaciones públicas que detallan los análisis realizados, las vulnerabilidades encontradas en el sistema y los posibles ataques.

- «Vot.Ar: una mala elección». Iván Barrera Oro y Javier Smaldone, Conferencia de Seguridad Informática Ekoparty, Buenos Aires, Argentina. 22 de octubre de 2015. https://www.youtube.com/watch?v=WcgslNiP3AQ
- Demostración del “puntero digital”. Javier Smaldone, Plenario de Comisiones de la Cámara de Diputados de la Nación Argentina. 4 de agosto de 2016. https://www.youtube.com/watch?v=XA3JZ2HWQuA
- «Una mala elección (actualizada)». Iván Barrera Oro y Javier Smaldone, Conferencia de Seguridad Informática Ekoparty, Buenos Aires, Argentina. 28 de octubre de 2016. https://www.youtube.com/watch?v=q3PVNIVUd28
- Detección remota de grabación con RFID. Alfredo Ortega y Javier Smaldone, Plenario de Comisiones del Senado de la Nación Argentina. 17 de noviembre de 2016. https://www.youtube.com/watch?v=Ay-r55E24zo

Referencias

[1] «Real-world Electronic Voting: Design, Analysis and Deployment», Feng Hao y Peter Y. A. Ryan (editores). ISBN 978-1-49-871469-3. Auerbach Publications, 2016. Capítulo 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». Enrique Chaparro. 2015. https://archive.org/download/voto-electronico-CABA

[3] «Vot.Ar: una mala elección». 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». CIPPEC, María Inés Tula (coordinadora). ISBN 950-9122-90-4. Editorial Planeta, 2005

TE DIC.
TECNOLOGÍA & COMUNIDAD