El sistema oculto en las máquinas de Vot.Ar

Javier

En la Ciudad Autónoma de Buenos Aires se ha implementado un sistema de voto electrónico que debería cumplir una serie de requisitos. Contrariamente a lo informado por la Justicia Electoral, el Gobierno y los medios de comunicación, el **sistema viola varios puntos de la ley**, su decreto reglamentario y las condiciones de licitación.

> *"Tanto la solución tecnológica, como **sus componentes de hardware y software** debe ser abierta e **íntegramente auditable** antes, durante y posteriormente a su uso".*
>
> (Artículo 24, inciso "b" del anexo 2 de la ley 4894 de la CABA)

> *"El contratista deberá proveer **al conocimiento y acceso, a los programas fuentes, funcionamiento de las máquinas de votación, sus características y programas (tanto hardware como software)**".*
>
> (Inciso 3.4.1, ítem 2, del pliego de la licitación pública 2-SIGAF-2015 de la CABA)

> *"La máquina de votación **no debe tener memoria ni capacidad de almacenar** el registro de los votos".*
>
> (Anexo I, artículo 24, inciso "p" del decreto 376/014 de la CABA)

> *“El dispositivo electrónico de emisión de voto y escrutinio […]* ***no debe tener memoria ni capacidad de almacenar*** *el registro de los votos”.*
>
> (Inciso 3.5.2 del pliego de licitación pública 2-SIGAF-2015 de la CABA)

> *“Ponemos un equipo,* ***una máquina absolutamente boba****, que no tiene disco rígido, que no tiene memoria,* ***que no tiene capacidad de almacenamiento alguno****“.*
>
> (Sergio Angelini, CEO y principal accionista de Grupo MSA)

> *“No tiene memoria la máquina,* ***porque es una impresora****“.*
>
> (Guillermo Montenegro, Ministro de Justicia y Seguridad del Gobierno de la CABA)

¿Una impresora o dos computadoras?

El sistema de voto electrónico (rebautizado *“boleta única electrónica”* en la CABA) **Vot.Ar** de la empresa MSA consta de una máquina que actúa, en una primera etapa, como emisora y, en una segunda, como contadora de votos. La empresa asegura que dicha computadora **no tiene ninguna capacidad de almacenamiento**, tal como lo exige el pliego de licitación. Además, MSA está obligada a **proveer el software** a utilizarse a fin de la realización de auditorías.

Con respecto al software, unos días antes de la votación, la autoridad electoral convoca a los partidos políticos a que envíen a sus “fiscales informáticos” y, en un proceso conducido por los técnicos de la empresa, revisan el código fuente de la aplicación (tanto como esto puede hacerse en una pantalla y en un par de horas), y graban un DVD “maestro”. Luego, y siempre a la vista de todos, realizan tantas copias del DVD como mesas haya en la

elección, y las entregan a la Justicia Electoral para su custodia. No se verifica que ese código se corresponda con alguna versión previamente auditada y considerada estable, ni tampoco la autenticidad e integridad del restante software incluido en el DVD (sistema operativo y unos 600 programas). De esta forma, notoriamente insuficiente, **se intenta mostrar que la integridad del software que ejecutarán las máquinas de votación y conteo está garantizada**.

Lo que la empresa no dice, y ninguna de las auditorías publicadas aclara, es que **la máquina de votación no es una computadora, sino dos**. Una de ellas, la visible, es la que ejecuta el software que se encuentra en el DVD de arranque (digamos, el conjunto que ha sido parcialmente auditado). **La otra, de la que nada se comenta, ejecuta un software desconocido** para la autoridad electoral, los partidos políticos y el público en general, en clara violación de la ley y su decreto reglamentario.

Esta segunda computadora se encarga, ni más ni menos, de gestionar el dispositivo de lectura y escritura de los chips RFID incluidos en las boletas, además de la impresora. En ella, se ejecutan **un sistema operativo y un programa que no sólo no son mencionados en las auditorías**, sino que escapan hasta al limitado escrutinio que se permite a los fiscales informáticos partidarios.

Para agravar la situación esta segunda computadora, contraviniendo el decreto reglamentario de la ley, los términos de la licitación y la palabra de la empresa, **sí tiene capacidad suficiente para almacenar** cuando menos los identificadores únicos de cada chip RFID, el número de secuencia, la hora de emisión (grabación) y el contenido de cada voto. Recordemos que por este subsistema pasa **todo lo que es escrito en (o leído de) los chips de las boletas de votación y lo impreso en las mismas**, y de almacenarse esta información podría **violarse el secreto del voto**.

Y para aumentar aún más las sospechas sobre el sistema, al menos en los modelos que hemos podido verificar, se encuentra presente un cable (accesible en la parte inferior del chasis de la máquina de votación) **mediante el cual sería posible acceder a la información guardada en esta segunda computadora, como así también modificar su software**, en cuestión de segundos.

Descripción técnica

La arquitectura

La máquina de votación está compuesta por **dos subsistemas principales**: uno basado en un procesador Intel (Celeron o Atom, según el modelo), que ejecuta una versión del sistema operativo Ubuntu y sobre éste la aplicación Vot.Ar (escrita principalmente en Python y Javascript), y otro basado en un procesador ARM que ejecuta **un sistema operativo desconocido** (posiblemente chibiOS o FreeRTOS) sobre el cual corre **una aplicación cuyo código también se desconoce**.

El subsistema ARM

El procesador ARM se encarga de gestionar el lecto/grabador RFID ISO/IEC 15693 y la impresora térmica. Es accesible al subsistema anterior como un dispositivo serial, a través del dispositivo *"ttyACM0"* en Linux (como puede apreciarse en el módulo armve del software Vot.Ar). En los modelos analizados, se trata de un chip Atmel AT91SAM7X256, como puede observarse en la siguiente imagen:

Según las especificaciones del fabricante, **dicho chip posee una memoria flash (de almacenamiento permanente) integrada de 256 Kbytes** suficiente para almacenar (además del sistema operativo y la aplicación) la información de los votos emitidos en más de una mesa.

Según la documentación del chip Atmel AT91SAM7X256, este

puede ser programado (incluyendo la lectura y grabación de su memoria flash) **a través de una interfaz JTAG**.

Además, mediante el “security bit” puede **impedirse el acceso al software almacenado en el chip** (que podría utilizarse además de violar el secreto para ciertas formas sutiles de fraude).

El cable JTAG

El chasis con forma de valija de las máquinas de Vot.Ar evidencia un cuidadoso diseño: cada elemento está debidamente colocado y sujetado mediante guías dispuestas a tal efecto. No se observa en el conjunto ningún elemento que no cumpla una función específica. La parte del chasis que actúa como base del equipo, posee 5 cavidades cubiertas por tapas de color negro. En las 3 cavidades inferiores se ubican los dos packs de baterías y la fuente de alimentación para conectar el equipo a la red eléctrica.

En el compartimiento superior izquierdo, según la imagen anterior, en los equipos analizados se encontró lo siguiente:

Los cables que vienen de la parte superior y que van hacia abajo y hacia la derecha, son los que transportan la energía eléctrica desde las baterías y desde el transformador. Llama la atención **un cable que finaliza con un conector en esta cavidad**. Siguiendo el recorrido de estos cables, a través de la bisagra del chasis y hasta la parte superior, observamos lo siguiente:

Tanto los cables de potencia como el cable no identificado van conectados al motherboard del equipo. Los de electricidad en un conector de alimentación, y el restante **en un conector etiquetado como “JTAG”**.

¿Se utiliza este cable para programar/leer la memoria del chip ARM? ¿Cuál es el objetivo de colocarlo de forma accesible en la base del equipo? ¿Se encuentra también en las máquinas

utilizadas en las votaciones oficiales?

Conclusiones

- El sistema está compuesto por **dos computadoras independientes**, cada una de las cuales ejecuta un sistema operativo y aplicaciones sobre él.

- El sistema basado en el procesador ARM **tiene capacidad de almacenamiento permanente**, suficiente para almacenar la información de los votos de más de una mesa.

- El sistema basado en el procesador ARM **no ha sido auditado** (ni su hardware ni su software).

- El software (sistema operativo y aplicación) que se ejecuta en el procesador ARM **no ha sido puesto a la vista de la Justicia Electoral**, ni de los auditores, ni de los fiscales informáticos de los partidos políticos.

- Llama la atención la colocación de un cable JTAG, accesible en la base del equipo, que podría servir para **acceder a la memoria de almacenamiento permanente** del sistema ARM.

Claramente, las máquinas de votación Vot.Ar —y al margen de otros cuestionamientos más profundos— **incumplen tanto la ley electoral de la CABA como su decreto reglamentario**.

Actualización (19 de julio de 2015)

El presidente de la mesa 2188 **pudo verificar la existencia del cable JTAG** en la máquina de votación asignada a la misma.

Además, el presidente de mesa **labró un acta** que será elevada a la Justicia Electoral, cuyo texto dice:

> *“Se hace constar que en uno de los compartimentos de la base de la máquina de votación número XX-XXXX-XXXX, puede observarse un cable negro grueso con un conector blanco con 8 (ocho) hilos o cables”.*

Al menos otros cuatro presidentes de mesa hicieron la misma comprobación, **también con resultados positivos**.

Adenda: La licitación de la CABA

El día 9 de febrero de 2015 se publicó en el Boletín Oficial de la CABA la evaluación de las propuestas presentadas por las empresas **MSA** y **Smartmatic**. En el ítem referido a *“ajuste del sistema al circuito del sistema de votación tradicional”* es donde se observó la mayor diferencia entre ambos oferentes: a **MSA** se le otorgó el máximo puntaje, en tanto que **Smartmatic** obtuvo un puntaje nulo. La razón que se adujo fue que el sistema de esta última *“posee instalado un disco rígido, […] como así también la existencia de espacio disponible para almacenar información”*.

Finalmente, se disparan en el pie afirmando que, por tener capacidad de almacenamiento, no se considera como un sistema de ***“boleta única electrónica”***, sino de ***“voto electrónico”***.