Prof. Claudio Enrique Righetti
Departamento de Computación – Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires
Pabellón I – Ciudad Universitaria – (C1428EGA) – Buenos Aires – Argentina
Tel./Fax:+54-11-4576-3359 - claudio@dc.uba.ar

OAT N° 03/15 – Auditoría de sistemas Elecciones 2015 – Ciudad de Buenos Aires

INFORME 3: Avance y Observaciones del sistema para voto con boleta única electrónica (BUE) al lunes 09/06/2015

Resumen ejecutivo

El presente informe complementa y continúa el **INFORME 2** de fecha 1° de junio y contiene las conclusiones y observaciones de lo analizado durante el período comprendido entre dicha fecha y el 9 de junio.

En este informe se analizan aspectos de seguridad, aspectos relacionados con los procedimientos y cambios informados o implementados por la empresa.

Cambios introducidos en el funcionamiento

En base a recomendaciones del Tribunal y luego de conversaciones mantenidas entre el equipo de Auditores y la empresa, esta última introdujo una modificación en el funcionamiento del software de la máquina de votación en lo relativo al acceso que se logra con la credencial de técnico. Con esta modificación para permitir al técnico cambiar el estado de la máquina se requiere de la participación de la autoridad de mesa.

En la nueva versión, una vez que la máquina está en funcionamiento en el modo de votación, la credencial de técnico no permite hacer nada (la misma es ignorada cuando se acerca al lector). En este modo, la credencial de autoridad de mesa lleva a la pantalla de inicio; al volver apoyar la credencial de autoridad el sistema solicita o bien cargar el número de mesa con el PIN o apoyar el Acta de Apertura de la mesa para luego habilitar la pantalla del menú principal.

Recién en este instante, sólo en este menú, y estando presente la autoridad de mesa responsable con su credencial y el PIN correspondiente y/o el Acta de Apertura, el técnico puede acercar su credencial y tener acceso a la pantalla de mantenimiento que lo habilita a cambiar los parámetros operativos (que, de todos modos, no permiten modificar el funcionamiento básico de selección de listas o candidatos e impresión de las BUE).

Aspectos de seguridad

Las tareas de revisión de los aspectos de seguridad realizadas hasta el momento se centraron en los siguientes aspectos:

1. Lectura del contenido del chip del voto, desde el momento de ser grabado y antes de ser introducido en la urna (afecta la *privacidad* del voto[1]).
2. Modificación el contenido del chip de voto (afecta la *integridad* del voto[2]).
3. Alteración del contenido de la máquina de votación para que se comporte de una manera distinta a la especificada[3].

Análisis de los aspectos de seguridad

Se analizaron diversas posibilidades de *ataque* al sistema buscando puntos débiles factibles de ser vulnerados para luego comparar dicha "*vulnerabilidad*" con el sistema de voto tradicional en papel con sobre y para analizar las medidas implementadas o implementables para mitigar o controlar dichas vulnerabilidades de modo tal que la misma ya no sea factible o su implementación no empeore el caso análogo en la elección tradicional con boleta de papel y sobre.

I. Lectura del contenido del chip del voto, desde el momento de ser grabado y antes de ser introducido en la urna

La lectura del contenido de la boleta podría violar el secreto del voto si la lectura se logra antes de meter la boleta en la urna de modo tal de saber cuál es el elector que votó con esa boleta. Entendemos que esto se puede realizar de dos maneras:

a) apoyando un celular moderno de tipo *smartphone* con soporte de NFC[4] (y software específico para esta tarea) a la boleta (o acercándolo a pocos centímetros de la misma). Dada la corta distancia necesaria para hacer esto[5], y el hecho de que la máquina está a la vista de las autoridades de mesa y fiscales, esta acción sería visible para dichas autoridades, los fiscales y el mismo elector, en especial si la operatoria se realiza en forma repetida;

---

1 Ley 4894, Anexo II, Art. 24, inc. p
2 Ley 4894, Anexo II, Art. 24, inc. e
3 Ley 4894, Anexo II, Art. 24, inc. q
4 NFC: Sigla de "*Near Field Communication*" que se puede traducir como "Comunicación de Campo Cercano". Es una tecnología que permite a teléfonos celulares y otros dispositivos conectarse entre sí utilizando comunicaciones de radiofrecuencia. Es posible utilizar esta tecnología para leer y escribir *chips* del tipo RFID desde un teléfono celular con soporte de dicha tecnología y software apropiado. El campo de acción de este mecanismo es usualmente menor a 10 centímetros, especialmente cuando la comunicación se realiza contra un *chip* RFID que no tiene alimentación propia.
5 Para poder hacer la lectura de la BUE vía NFC desde un *smartphone*, la boleta debe estar prácticamente apoyada sobre el mismo, ciertamente a una distancia bastante menor a los 10 centímetros y durante más de medio segundo, usualmente más de un segundo.

b) usando una antena especial con un dispositivo tecnológico que lea la máquina en el momento en que se está realizando la grabación del chip. Esos equipos especiales requieren una antena de algunas decenas de centímetros de longitud. Para mitigar este problema hay que extremar los controles de los ambientes de votación para impedir que personal ajeno a la elección manipule dispositivos electrónicos en cercanía de las máquinas de votación. Se han publicados trabajos donde se podría, en un ambiente libre de obstáculos, detectar señales hasta 18 metros de distancia. Las experiencias que probaron decodificar la señal de la máquina de votar de MSA lograron resultados para decodificar la señal emitida a 30 centímetros; a distancias mayores, la señal era detectable pero no se pudo decodificar.

   Tanto en los casos prácticos ensayados, como en las publicaciones teóricas, la detección de las señales se realizó dentro del mismo recinto (sin paredes u otros obstáculos) y la decodificación sólo es posible si la señal proviene de una sola máquina.

II. Modificación del contenido de la BUE

La modificación del voto, una vez emitido para reemplazar la información *impresa* en la BUE no es factible dado que la impresión es térmica y quema la superficie de la misma. No es posible modificar o *borrar* lo impreso.

Alterar el contenido del *chip* RFID para cambiar la información tampoco es factible porque los sectores utilizados para la grabación de la información son "*cerrados*" para que no puedan volver a escribirse. No se ha logrado modificar la información en *chips* que se hayan *cerrado* previamente.

Existe un tipo de *ataque* posible que sí podría hacerse consistente en *anular* la información contenida en el chip, impidiendo leer en el momento del escrutinio la información grabada. Para poder hacer esto se necesita un dispositivo que emita un pulso electromagnético fuerte. Se comprobó que las BUE son susceptibles a tal pulso utilizando un dispositivo casero. De todos modos este ataque no compromete el secreto del voto ni impide ejercer la voluntad del votante, generando un obstáculo (que no es insalvable) en el momento del escrutinio. Se recomienda tomar las mismas medidas para la observación anterior en relación al control de la presencia de personas ajenas o de personas manipulando dispositivos electrónicos en el área donde se encuentra la mesa de votación.

III. Alteración del contenido de la máquina de votación para que se comporte de una manera distinta a la especificada

La máquina de votación tiene una serie de puntos débiles en relación a la falta de control de los dispositivos internos (que podrían estar validados por claves y

certificados internos o adecuados niveles de permisos[6]). Para explotar cualquiera de esas debilidades se necesita acceder a la puerta superior, abrir el lector de DVD, cambiarlo por otro modificado especialmente y reiniciar el equipo. Esto hace que la custodia de la tapa superior de la máquina y tener la máquina a la vista de las autoridades de mesa durante todo el acto electoral sea la forma de controlar estas vulnerabilidades. Esta es una de las razones por las cuales se recomendó en el informe anterior cómo debe ser la disposición de la máquina de votación dentro del establecimiento.

De no controlarse la tapa superior de la máquina podría introducirse un DVD que cambie el comportamiento de la máquina de votación[7] pudiendo por ejemplo emitir votos distintos a los seleccionados o grabar información en el *chip* distinta de la impresa. Aún consiguiéndose esto, las anomalías en los votos son detectables en el momento de la verificación del voto o del proceso de escrutinio.

Otra cosa que podría hacerse es, además de cambiar el DVD, introducir un dispositivo USB con una memoria que registre los votos en orden o una antena que los transmita en el momento. Esto no es detectable por anomalías en el voto pero sí es detectable por la presencia física de un elemento extraño. De todos modos, para que el dispositivo USB funcione, también es necesario cambiar el DVD y reiniciar, o reiniciar y utilizar un teclado (también conectado a un puerto USB) para permitir que la máquina cargue el sistema operativo desde el dispositivo USB en lugar del DVD.

Recomendamos que las autoridades de mesa custodien la tapa de la máquina cuando los electores se aproximan a la máquina (para verificar que no se abre la tapa) y que periódicamente revisen que no haya dispositivos agregados en los puertos USB.

Conclusiones sobre los aspectos de seguridad

Es importante que, del mismo modo que ocurre en los operativos de elecciones tradicionales, se custodien los materiales que se despliegan en los establecimientos para que los mismos no sean manipulados por extraños. A los materiales tradicionales (urnas, boletas, padrones, etc) ahora se agrega la custodia de las máquinas, BUEs, DVDs, credenciales y actas de apertura y cierre.

6
a) procesos internos que corren en la máquina de voto utilizando permisos de *root*,
b) puertos USB expuestos físicamente (pero bajo la tapa superior y apagados por software)
c) BIOS sin contraseña y ausencia de control de actualización de la misma
d) ausencia de control de la validez del sistema operativo
e) ausencia de control de la validez del firmware

7 Para que este DVD funcione, sin embargo, es necesario reiniciar la máquina, lo cual emite una serie de pitidos y, por otra parte, demora en el orden de cinco (5) minutos, lo cual lo hace extremadamente difícil de realizar sin que sea advertidos por las autoridades o los fiscales.

Similarmente a lo que ocurre en una votación en papel, el despliegue de dispositivos tecnológicos disimulados u ocultos, ubicados en lugares estratégicos podrían filmar o fotografiar los movimientos de los electores de una mesa violando el secreto del voto o introduciendo un mecanismo para verificar el cambio de su voluntad. Es por eso que el control de las instalaciones, del establecimiento y de las personas que tienen acceso al mismo sigue siendo igual de importante cuando se introducen aspectos tecnológicos durante la emisión del voto.

Respecto de la custodia de la tapa superior de la máquina, recomendamos evaluar distintas alternativas que permitan, junto a la custodia de la misma por parte de las autoridad de mesa, detectar la apertura de la misma por parte de personas no autorizadas, ya sea mediante una señal sonora que se emita al abrir la tapa o un adhesivo de seguridad que la autoridad de mesa pegue luego de insertar el DVD.

El adhesivo puede estar dispuesto para impedir o detectar la apertura de la tapa superior o, mejor aun, debajo de la misma, uno para impedir o detectar la apertura de la bandeja del DVD y otro para tapar los puertos USB. En caso de ser necesario el acceso a la unidad de DVD por algún motivo, el presidente puede romper el adhesivo y luego colocar uno nuevo antes de continuar con el proceso de votación.

Se recomienda, asimismo, agregar al kit de la autoridad de mesa un marcador indeleble para que la autoridad de mesa firme el DVD antes de insertarlo en la máquina de votación y sea capaz de reconocer fácilmente si el mismo ha sido cambiado.

Se recomienda también que la autoridad de mesa no permita que los fiscales, electores u otras personas que estén en el recinto manejen teléfonos celulares u otro tipo de dispositivos en forma sospechosa, ya sea acercándolos a la urna, o a las BUE, especialmente cuando los electores regresan de la máquina. La utilización “normal” de los teléfonos, ya sea para hablar o enviar y recibir mensajes de texto no interfiere en el normal funcionamiento del comicio.

Tampoco es recomendable que se utilicen los teléfonos para grabar o filmar dentro del recinto de voto (esto también se aplica al proceso tradicional con boleta de papel y sobre).

Estas recomendaciones, salvo la custodia de las máquinas y DVDs, no son de carácter obligatorio para asegurar el comicio; pero su cumplimiento, o la de otras alternativas equivalentes, mejoran la seguridad del mismo.

Como se indicó en las conclusiones del **INFORME 2** de fecha 1° de junio, la auditoría sostiene que el sistema permite respetar los principios enunciados en el Artículo 24 del Anexo II de la Ley 4894.