DVT 56-504: Auditoría de Sistema de Votación Electrónica 2015 para la Defensoría del Pueblo de la C.A.B.A.

Informe de Auditoría

1. Contexto General

La Defensoría del Pueblo de la C.A.B.A. ha solicitado una auditoría sobre el sistema de voto con boleta única electrónica a utilizarse en las Elecciones 2015 de la Ciudad Autónoma de Buenos Aires.

El análisis para la auditoría fue realizado sobre una de las máquinas de votación en su versión para Capacitación, ubicadas en la sede de la Defensoría del Pueblo de la CABA, sito en Piedras 574, que operan únicamente en modo "Emisión de Votos", y un conjunto de Boletas Únicas Electrónicas para pruebas. También se consultaron los procedimientos publicados en el sitio http://www.votar.com.ar/ de la empresa MSA, la información publicada en el sitio http://www.buenosaires.gob.ar/boletaelectronica del Gobierno de la Ciudad de Buenos Aires, y el documento de la Acordada Electoral nº 17/2015 del Tribunal Superior de Justicia (en adelante, TSJ).

Oportunamente se nos informó que el hardware presentado y la versión software del sistema auditado no son necesariamente los que se utilizarán en la elección de la Ciudad de Buenos Aires el próximo mes de Julio.

Cabe mencionar que la aplicación de software está compuesta por varios módulos o componentes, alguna son de código abierto y otros no. Como en cualquier desarrollo de software con componentes, cuando alguna de las mismas se actualiza, impacta en la ejecución de aquellas otras que dependen directa o indirectamente de ellas. Respecto de ello es fundamental que no sólo la aplicación sino cada una de sus componentes se encuentre versionada y que, ante la actualización de alguna de ellas, pueda realizarse una nueva auditoría sobre todas las componentes que dependen directa o indirectamente de ella, más en este tipo de aplicación donde la finalidad es crítica. De lo contrario, una actualización en alguna componente (inclusive provista por terceros) puede introducir riesgos importantes en el sistema.

2. Limitaciones a la Auditoría

Las circunstancias que se describen a continuación no nos permitieron aplicar todos los procedimientos necesarios para auditar en forma completa el Sistema de Votación Electrónica:

- La máquina sobre la que se realizó la auditoría sólo operaba en modo "Emisión de Votos", por lo cual no se pudieron auditar los módulos correspondientes a Apertura de Mesa, Cierre de Mesa y Escrutinio, y Emisión de las Actas de Mesa. Tampoco se puedo relevar la Carga de Resultados de mesa y transmisión de datos.
- No se tuvo acceso a información sobre el hardware, más allá de lo que se relevó visualmente.
- No estuvo disponible ni el código fuente, ni la Arquitectura del sistema, ni el manual de procedimientos de la empresa MSA.

2. Relevamiento

A continuación se enumeran algunos aspectos que se han detectado en el relevamiento realizado, conforme al material detallado en el punto 1.

2.1. Relevamiento sobre Funcionalidad

Dado que no se contaba con el código fuente, y la máquina sólo operaba en modo Emisión de Votos, sólo se pudo realizar una prueba de caja negra de funcionalidad de dicho modo, con la intención de evaluar su comportamiento ante posibles errores, por parte de los votantes, en el uso del software y de la Boleta Única Electrónica (en adelante BUE).

El sistema fue testeado con múltiples votaciones, tanto de voto por lista completa como de voto por categorías. De dichas pruebas no se detectaron incoherencias entre la votación grabada en el chip RFID y la votación impresa salvo ante el retiro anticipado de la BUE de la máquina. A continuación se detalla dicha situación, la cual introduce tres tipos de errores.

Cuando el votante ingresa la boleta, elige un candidato, cliquea el botón de aceptar y retira la BUE anticipadamente, aunque aparezca un cartel indicando "no retire la boleta", se producen tres tipos de errores, según el momento del proceso en el cual el usuario retira la boleta, a saber:

2.1.1. Si al retirar la BUE, la máquina ha iniciado la grabación del chip RFID pero no la ha finalizado, el sistema ya no responde y se tiene la necesidad de reiniciar la máquina.

2.1.2. Si al retirar la BUE, la máquina ha finalizado la grabación del chip RFID, entonces queda una boleta con el voto registrado sólo en el chip RFID, sin el voto impreso en la boleta. Esto impediría contrastar el voto grabado en el chip RFID con el voto impreso que se puede visualizar fácilmente en la BUE.

2.1.3. Si al retirar la BUE, la máquina ni siquiera ha iniciado la grabación del chip RFID, entonces al volver a ingresar para un nuevo voto, en la pantalla se muestra la selección del votante anterior ("recuadrado en verde"). Esto es, aparece un candidato preseleccionado y se observa visualmente lo que el usuario anterior eligió. En caso de que el usuario solicitara ayuda a alguna autoridad de mesa, la misma visualizaría la elección realizada por el votante, pasando a una situación donde se violaría el secreto del voto.

2.2. Relevamiento sobre Procedimientos

De la información pública disponible citada en el punto 1, pudimos relevar que las boletas cuentan con un número serializado único dentro del chip RFID. Esto implica que teniendo el equipo apropiado (un teléfono celular, por ejemplo) se puede identificar una boleta antes de votar y luego, durante el recuento, con el voto ya impreso. Si esta identificación fuera asociada a un votante en particular, se estaría violando el secreto del voto.

Se pudo verificar que cuando el votante emite su voto, el mismo queda registrado en la BUE de dos formas diferentes: almacenado en el chip RFID e impreso en la boleta. Queda claro que sería un problema grave que ambas informaciones no fueran coincidentes, aunque queda a voluntad del votante verificar que el voto impreso coincida con el voto almacenado en el chip RFID.

En relación con el párrafo anterior, tampoco se puede asegurar que, aunque el votante verificara la coincidencia entre el voto almacenado en el chip RFID y el voto impreso en la boleta, a través de la misma máquina en la cual está votando, dicha coincidencia sea efectiva. Es decir, no se puede asegurar que la máquina muestre el voto por la lectura efectiva del chip RFID y no por datos del programa almacenados temporariamente. Es más, aunque en modo "Emisión de Votos" se verifique la coincidencia, tampoco queda asegurado que la misma siga manteniéndose al ser chequeada en el modo "Escrutinio".

Por otra parte, dado que el conteo digital es sólo un escrutinio provisorio el cual será comparado con el escrutinio definitivo realizado a través del conteo de las boletas impresas en el soporte papel, y dado que si no hay impresión en la boleta se computa como Voto Nulo (Ver Art 7. Del Anexo II de la Acordada 17/2015), existiría un serio problema si ocurriera la situación descripta en los puntos 2.1.1, 2.1.2 y 2.1.3.

Cabe señalar que, por la naturaleza de RFID, los chips de las BUEs pueden llegar a ser alterados individual o masivamente. Los chips utilizados en la capacitación permiten escrituras sucesivas, pero en esta auditoría no se tuvo acceso al tipo de chip RFID definitivos que se utilizará efectivamente en el acto electoral.

Si existe un plan alternativo del proceso de votación en caso de una falla total del sistema en alguna sede, el mismo no fue verificado por esta auditoría.

2.3. Relevamiento sobre Seguridad

Al inspeccionar el hardware, se pudo notar que la máquina auditada ofrecía libre acceso a la lectora de DVD, a la placa de red y a sus cuatro puertos USB. En apariencia, la misma no tiene un sistema ya cargado, sino que se debe iniciar con un DVD que se coloca en el acto de apertura de la mesa.

Aunque en cada sede desde una máquina se transmiten los resultados de las actas de dicha sede, no se pudo auditar la transferencia de la información hacia el centro de cómputos, ni los protocolos que se utilizarán para la misma.

3. Conclusiones

En base al análisis realizado sobre las componentes auditadas del sistema, y atendiendo a las limitaciones estipuladas en el punto 2, se sugiere fuertemente las recomendaciones que se enuncian a continuación.

- Respecto del sistema en su totalidad:

Recomendación 1: Se debe auditar el sistema completo (hardware, software, comunicación) definitivo a instalar en las máquinas de

votación, con anterioridad a los comicios. **Una vez que el TSJ (o quien el tribunal disponga) haya auditado el hardware y el DVD con la versión definitiva, la empresa ya no debería introducir ningún cambio en el sistema, sin volver a ser auditado en su totalidad**. Es aconsejable que exista una sola versión del sistema, pero en caso de que haya más de una versión para el acto electoral, todas ellas deberían ser auditadas en forma completa.

- Respecto a la Etapa de Votación:

Recomendación 2: Se recomienda que las autoridades de mesa no entreguen al votante la boleta (a diferencia de lo expresado en el Art. 2 del Anexo II de la Acordada 17/2015). Se sugiere **establecer y difundir políticas de difusión para que los votantes conozcan su derecho de elegir una BUE a partir de un conjunto de boletas ubicadas sobre la mesa de votación.** Con esto se disminuye la posibilidad de asociar una boleta con un votante.

Recomendación 3: Dado que por el Art. 7 del Anexo II de la Acordada Electoral 17/2015, el voto sin impresión en la BUE es considerado Voto Nulo, se sugiere fuertemente **establecer y difundir políticas de recomendación a los votantes para que verifiquen que el voto realmente está impreso en la boleta antes de entregar la misma.**

Recomendación 4: El Artículo 7 del Anexo II de la Acordada 17/2015 debería ser extendido para **aclarar explícitamente cómo considerar la situación donde hay impresión visible en la BUE, hay lectura del chip RFID (no se trata de un voto no leído por motivos técnicos), pero los datos no coinciden.**

Recomendación 5: Se sugiere fuertemente establecer y difundir políticas de recomendación a los votantes para que realicen la verificación de la coincidencia entre el voto almacenado en el chip RFID leído por la máquina y el impreso en la boleta, antes de entregar su boleta en la mesa.

Recomendación 6: Adicionalmente a la recomendación 5, también se recomienda que el votante emita el voto en una máquina pero realice la verificación de lo votado en otra máquina, antes de entregar la boleta con el voto realizado. Se sugiere que en cada sede haya una o más maquina en modo "Escrutinio" para este fin, pero que no almacenen ni sumen resultados.

Recomendación 7: Las máquinas no deberían permitir el fácil acceso a los puertos externos USB, ni a la placa de red, ya que los mismos presentan un punto de acceso vulnerable. De no poderse subsanar dicha exposición, se recomienda que las máquinas sean colocadas de manera tal que se encuentren siempre a la vista de las autoridades de mesa y fiscales, para minimizar los riesgos de los accesos físicos indebidos. Cabe señalar que dicha visualización debe realizarse de manera tal de asegurar que se observe el acceso a los puertos, pero no se visualice la pantalla en la cual realiza su voto el elector.

Recomendación 8: Dado que el retiro anticipado de la boleta genera varias situaciones problemáticas (llevando a voto nulo por la falta de impresión en la BUE), **se recomienda reemplazar el cartel que se despliega indicando "no retirar la boleta", por un mecanismo que realmente no permita hacer esta acción,** como por ejemplo, que la misma quede absolutamente dentro de la máquina (inaccesible a las manos de un usuario,) tal como ocurre con algunos cajeros ATM de

bancos. Al finalizar la grabación del chip RFID y de la inscripción de la boleta, la máquina debería proceder a expulsarla.

- *Respecto de la Etapa de Escrutinio:*

Recomendación 9: Al momento del escrutinio es recomendable cotejar el dato impreso con el digital, con lo cual se puede aportar verificación al sistema electrónico. Aunque en la Acordada 17/2015 se indica que cuando una BUE no puede ser leída por la máquina se considera como "voto no leído por motivos técnicos", falta discriminar el procedimiento a seguir si el voto impreso no coincidiera con el leído electrónicamente.

- *Respecto de Transmisión de Resultados*

Recomendación 10: La comunicación entre la máquina que realiza la conexión con el centro de cómputos tiene que seguir los más altos estándares de cifrado SSL/TLS utilizando certificados de al menos 2048 bits que permitan cifrado de 256 bits. Se deberían utilizar tanto certificados para validar el servidor como también para validar el cliente. El no seguir esta recomendación implica que la información puede ser adulterada por terceros durante su transmisión.

Ciudad Autónoma de Buenos Aires, 9 de Junio de 2015

Departamento de Informática
Instituto Tecnológico de Buenos Aires