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 5: Observaciones del sistema de voto con boleta única electrónica (BUE) para la segunda vuelta al viernes 17/07/2015

Resumen ejecutivo

El presente informe complementa y continúa el **INFORME 4** de fecha 23 de junio y contiene las conclusiones y observaciones de lo analizado durante el período comprendido entre dicha fecha y el 17 de julio.

En este informe se analizan cambios informados o implementados por la empresa así como algunos datos acerca del desempeño del sistema durante las elecciones generales del 5 de julio.

Aspectos funcionales del software

Llamamos aspectos funcionales del software a las características del mismo que son visibles por los usuarios o que determinan qué es lo que el usuario puede hacer y cómo.

Son usuarios del software:

- Los ciudadanos en general en su rol de electores y autoridades de mesa en las máquinas de votación.
- Las autoridades electorales que deben poder tomar decisiones sobre ciertos aspectos del proceso, así como sus delegados en los sitios de votación.
- Los partidos políticos en su rol de fiscales.

El software debe, en forma clara y eficiente, permitir a los usuarios realizar sus tareas. Debe proveer los mecanismos de control posibles para minimizar los errores provenientes del uso del mismo.

Cambios introducidos en el funcionamiento del sistema

Dado que en la segunda vuelta sólo se elige una categoría (Jefe y Vicejefe de Gobierno), desapareció la pantalla inicial que permite votar por lista completa o por categorías, del mismo modo que no hay botones individuales para modificar la selección una vez hecha, sino un solo botón rojo que vuelve a la única pantalla de selección.

En la segunda vuelta no hay consulta popular y la elección por Jefe y Vicejefe de Gobierno es para todo el distrito, por lo cual las pantallas son idénticas en todas las Comunas.

Se verifica que, de acuerdo a la decisión del Tribunal en la Audiencia del día 8 de julio, la pantalla de selección ahora contiene los candidatos de las dos agrupaciones que participan de la segunda vuelta (siempre en orden aleatorio), con una franja que atraviesa toda la pantalla debajo de los datos de ambas listas para votar en blanco.

Si se oprime la opción "Modificar" luego de seleccionada alguna de las tres opciones, a diferencia de lo que ocurría en la primera vuelta, no aparece resaltada en color azul la selección anterior, sin embargo, dada la escasa cantidad de opciones y el hecho de que es una sola categoría, no estimamos que la ausencia de este resaltado sea significativa.

Observaciones sobre la funcionalidad

Las observaciones sobre la funcionalidad reportadas en el Informe 4 que siguen siendo relevantes para la segunda vuelta siguen en su mayoría en el mismo estado. En particular las observaciones 4, 6, 7, 10 y 20 siguen en el mismo estado que estaban para las elecciones generales del 5 de julio pasado.

Nueva observación: Para salir del modo "demo" es necesario acercar dos veces seguidas la credencial de autoridad de mesa. Esto es confuso. En la versión utilizada para las elecciones generales acercando la credencial de autoridad al lector mientras estaba en modo "demo" volvía a aparecer el selector de comuna de dicho modo, y si se acercaba nuevamente la credencial de autoridad de mesa volvía a la pantalla de inicio al sistema.

Es posible que, habiéndose eliminado el selector de Comuna del modo "demo", al acercar la credencial a la pantalla se produzca un error que no se está atrapando y está enmascarado según se consignó en informes anteriores.

De todos modos, como se consignó en el Informe 4, si las máquinas para capacitación y demostración utilizarán una versión diferente del software, el modo "demo" debería estar completamente deshabilitado en las máquinas de voto.

Código fuente auditado

La última entrega de código fuente por parte de la empresa MSA a esta auditoría antes de las elecciones del 5 de julio fue hecha el 17 de junio. Dicho código fue el que se utilizó durante dicho acto en las máquinas de voto (esto fue verificado por los auditores), sin embargo, el software para la transmisión de actas de escrutinio sufrió modificaciones entre el 17 de junio y la duplicación de DVDs de transmisión

realizada el 1° de julio, del mismo modo que hubo modificaciones en el software de recepción de dichas transmisiones que corre en los servidores.

Las versiones definitivas del código fuente con el software para ser utilizado en la segunda vuelta fueron recibidas el sábado 11 de julio, con menos de cuatro días para ser auditado antes de la fecha pautada para la entrega del presente informe, miércoles 15 de julio.

Los auditores encontraron una gran cantidad de cambios más allá de las configuraciones: en el orden de 10.000 líneas borradas o agregadas en casi 200 archivos. Esto es en sí mismo una debilidad del código fuente como cualquier cambio en partes extensas del software a pocos días de la puesta en producción. que sea imposible revisar la totalidad de los cambios en tan corto tiempo. En el Anexo I se realizan algunas observaciones específicas sobre parte del código fuente que la presente auditoría entiende son significativas del sistema. Gran parte de las observaciones sobre el código hechas en informes anteriores siguen estando vigentes.

Aspectos de seguridad

Durante las semanas previas a las elecciones generales del 5 de julio se publicaron algunas supuestas vulnerabilidades halladas en el sistema; detallaremos a continuación las que nos parecen más significativas.

Publicación de información sensible

Luego de una prueba de despliegue y transmisión realizada el 20 de junio por la empresa en los establecimientos, se publicaron datos de los certificados SSL de cliente utilizados durante dicha prueba para transmisión de datos así como PINes de autoridad de mesa y datos personales de los técnicos contratados por la empresa para el operativo.

Aparentemente estos datos habrían sido obtenidos mediante un ataque al sistema de operaciones que utiliza la empresa (que está fuera del alcance de la presente auditoría).

De todos modos, más allá de la publicación de datos personales de los técnicos, no se consideró que estuviera en peligro el operativo de elecciones por los siguientes motivos:

- Los certificados SSL de cliente se cambian para cada operativo (es decir, los que se utilizaron durante la prueba del 20 de junio no eran los mismos que se utilizarían el 5 de julio).

- Los PINes por sí mismos no alcanzan para suplantar a una autoridad de mesa (y poder generar actas de apertura y cierre o escrutinio) si no que es necesario contar con una credencial con un chip RFID cuyo contenido no es posible generar sabiendo sólo el número de mesa y el PIN.

Finalmente, la empresa cambió el mecanismo de distribución y carga de certificados SSL de cliente que utilizó durante el operativo del 5 de julio minimizando considerablemente el riesgo de que la filtración de información producida el 20 de junio se repita.

"Multivoto"

El viernes 3 de julio la Fundación Vía Libre[1] publicó un documento[2] y un video[3] donde se muestra la utilización de una BUE con un voto grabado en el chip RFID que genera más de un voto en la misma categoría. Dicho documento denomina "multivoto" a dicha boleta.

El domingo 5 de julio, luego de las 18 horas, se publicó[4] también la forma de generar una boleta "multivoto"[5].

Para generar dicho voto es necesario grabar el chip RFID manualmente (por ejemplo, utilizando un smartphone con soporte de NFC y software apropiado) ya que el software de voto no genera más de un voto por categoría.

Dados los procedimientos y recaudos de votación, si un elector quisiese emitir su voto de este modo, no puede llevarlo preparado con anterioridad ya que las autoridades de mesa controlan que la BUE que se insertará en la urna es la misma que se le dio al elector en dicha mesa (controlada por medio del par de troqueles en dicha boleta).

Por ello, el elector debe grabar subrepticiamente el chip utilizando su teléfono mientras supuestamente está imprimiendo su voto en la máquina, más allá de poder hacerlo sin llamar la atención de las autoridades de mesa y los fiscales, si el elector graba la BUE con un "multivoto" *antes* de insertar la boleta en la máquina y luego la inserta, el software de la máquina reconocerá que la BUE no está "vacía" y la expulsará sin permitirle imprimir el voto. En este caso (o en el caso de que el elector jamás inserte la BUE en la máquina), el lado que debe imprimirse de la boleta quedará en blanco. Durante el recuento, dicha boleta será contabilizada como voto nulo sin ser apoyada en el lector, con lo cual no se contabilizará electrónicamente el

1 http://www.vialibre.org.ar
2 http://www.vialibre.org.ar/wp-content/uploads/2015/07/AtaqueMulti-VotoaSistemaVot.Ar_.pdf
3 https://www.youtube.com/watch?v=CTOCspLn6Zk
4 https://twitter.com/beabusaniche/status/617806242384363520
5 https://docs.google.com/document/d/1aJttB2w7ejuIKjSRGz_hKbuK4rMUueL5q_TYiCHfGOc

"multivoto" si no que se contará manualmente al finalizar el recuento con los demás votos nulos.

Si, por el contrario, el elector emitiera un voto cualquiera que imprima datos válidos en la BUE y después intentase grabar el "multivoto" utilizando su *smartphone* con NFC, dicha grabación sería imposible ya que la máquina, al grabar el voto habría "*cerrado*" el chip RFID impidiendo su modificación posterior.

Además el software de totalización realiza controles de consistencia y hubiera rechazado la información proveniente de una mesa con boletas alteradas de este modo; dicha inconsistencia no se habría incluido en el escrutinio provisorio y habría sido marcada para ser revisada manualmente en el escrutinio definitivo.

En el software de voto para la segunda vuelta, se agregaron controles para no contabilizar más de un voto por candidato durante el recuento hecho en la máquina.

Conclusiones

Más allá de ser necesarios para adaptar el sistema a la única categoría que se elige en la segunda vuelta o convenientes para el refuerzo de la seguridad frente a potenciales vulnerabilidades, los cambios realizados por la empresa alcanzan un número relativamente elevado lo que produjo el atraso en la entrega del presente informe.

Se mantiene la premisa expuesta en los informes anteriores de que es crucial para el correcto funcionamiento del sistema en forma global, que las autoridades de mesa, delegados judiciales y demás responsables de los comicios sigan los procedimientos aprobados por el Tribunal en el Anexo II de las Acordada 17/2015.

Esta auditoría considera que el sistema permite respetar los principios enunciados en el Artículo 24 del Anexo II de la Ley 4894.

En particular, el sistema es comprobable físicamente y la voluntad de los electores se puede verificar en forma completamente manual, sin la intervención del sistema informático; en casos extremos (aunque improbables) de fallas generalizadas o ante un requerimiento de fiscalización por parte de las agrupaciones políticas que se considere admisible.

Anexos

Anexo I – Observaciones sobre el código fuente

A continuación se detallan algunas observaciones, encontradas al revisar el código fuente del software, que son puntos débiles detectados. Si bien no son errores en sí mismos podrían serlo en determinados contextos. Esta auditoría no se encuentra en la capacidad de afirmar o negar la posibilidad de estos errores dado el estado actual de la documentación del sistema.

Cada observación descrita es un representante de uno de los tipos de observaciones encontradas, es decir, *no son los únicos extractos de código observados, sino una **tipificación** de los mismos*.

Los errores encontrados en el código que son visibles desde el punto de vista funcional son reportados en la sección de “Aspectos funcionales del software”.

1. **Fuente**: …`/msa/deploy/database/scripts/ddl/create/functions.sql`

   Función/sección/clase: `publicar`, líneas 332 a 334

   Contenido aproximado:

```
FOR rec_planilla IN cur_planilla LOOP
    -- Paso los votos a definitivos. Debería ser llamado desde Carga
    PERFORM pasa_votos_definitivos(rec_planilla.id_planilla);
```

   Observación: Se observa el uso de **`PERFORM`** dentro de las funciones almacenadas en la base de datos PostgreSQL. La instrucción `PERFORM` se utiliza para invocar funciones cuando no se necesita el resultado. El problema con el uso de `PERFORM` es que enmascara los errores de la función invocada (las excepciones lanzadas en la función son ignorados por el `PERFORM` impidiendo la propagación correcta del error).

   Posible solución: Utilizar un `SELECT INTO` en vez de `PERFORM` y si realmente se necesita omitir o ignorar alguna condición de error utilizar un bloque `EXCEPTIONS` haciendo explícita la condición de error que debe ignorarse (en lugar de ignorar todas).

2. **Fuente**: …`/msa/movil/fiscales/www/js/main.js`

   Función/sección/clase: `render_resultados`, línea 171

   Contenido aproximado:

```
$("#datos").html("<h3>Mesa: " + result.mesa.numero + "</h3>");
```

Observación: Se utilizar la función `html` de `jquery` (equivalente a la propiedad `innerHTML`) para establecer el texto de un elemento en pantalla con datos variables obtenidos de los parámetros de la función y/o de datos que directa o indirectamente tienen como fuente algún usuario del sistema. Esto hace el código susceptible a la inyección de código `HTML` y/o `javascript`. Si bien no se halló ningún caso en que esta vulnerabilidad pueda ser explotada directamente, el código así programado tiene una debilidad debida a no controlar los datos que se asignarán a como `HTML` al elemento en pantalla.

Posible solución: Utilizar una vía segura para el establecimiento de textos. Por ejemplo usar la función `text` de `jquery` (equivalente a la propiedad `textContent`). En este caso:

```
$("#datos").append($("<h3>").text(Mesa: " + result.mesa.numero));
```

O cuando se quiera enviar mensajes con algún tipo de formato (negritas, colores, estilos, etc) usar una función propia que solo permita datos que tengan los elementos `HTML` admitidos y seguros:

```
$('.status-' + dispositivo).html(control_html_admitido(mensaje));
```

(el último ejemplo está tomado de la función `set_status` en línea 27 de `…/msa/desktop/transmision/templates/js/transmision/funciones.js`).