.Seguridad
Cultura de prevención para TI
Publicado en *Revista .Seguridad* (http://revista.seguridad.unam.mx)

México, el voto electrónico y el 2012

Por *Gunnar Eyal Wolf Iszaevich*

numero-14[1] elecciones [2] simulacro [3] urnas electrónicas [4] voto [5] vulnerabilidades [6]

Tweet [7]

Un reclamo muchas veces escuchado es que, dado que es imposible confiar en los individuos, corruptibles por naturaleza, la responsabilidad del escrutinio de los votos debería recaer en un sistema computarizado, siempre limpio, eficiente y honesto. Las urnas electrónicas se han propuesto desde hace mucho tiempo y muchos países (o jurisdicciones menores) las han adoptado.

Un reclamo muchas veces escuchado es que, dado que es imposible confiar en los individuos,

corruptibles por naturaleza, la responsabilidad del escrutinio de los votos debería recaer en un sistema computarizado, siempre limpio, eficiente y honesto. De eso hablaremos a continuación.

¿Qué hace una urna electrónica?

Las urnas electrónicas se han propuesto desde hace mucho tiempo y muchos países (o jurisdicciones menores) las han adoptado.

En el corazón de todas las propuestas de voto electrónico está la *urna electrónica*. Esta es básicamente una computadora con una interfaz de usuario limitada para solo permitir un conjunto específico de operaciones, construida dentro de una caja o maletín que dificulte el acceso a cualquiera de sus componentes, fuera de aquel expresamente autorizado y encargado de recibir cada uno de los votos, convirtiéndolos en *información almacenada electrónicamente*. Por medio de un procedimiento previamente diseñado, las autoridades electorales pueden indicarle que deje de recibir votos y que entregue los totales que cada una de las opciones que capturó.

Las primeras urnas electrónicas que cumplen con esta definición, las llamadas *DRE voting machines* (*Direct-Recording Electronic*, máquinas de voto electrónico de grabación directa) fueron puestas en práctica ampliamente hacia 1996. Al día de hoy, votan de esta manera la totalidad del electorado de países tan grandes como la India y Brasil, así como amplios segmentos de otras naciones como los Estados Unidos.

La confianza y los aguafiestas

Si una cosa caracteriza al gremio de los desarrolladores de software es la cantidad de errores (tanto accidentales como inducidos, lo que es mucho más peligroso) que pueden aparecer en un programa, no lo

perdamos de vista. El mero hecho de que exista un área de especialización tan importante como la seguridad informática lo hace patente: La complejidad hasta de los sistemas más sencillos hace imposible asegurar *con toda certeza* que una computadora haga lo que debe hacer.

Para ilustrar: Son pocas las computadoras en el mundo que no utilizan una solución antivirus en la actualidad. Estos programas se hicieron necesarios dadas las grandes deficiencias de diseño que tuvo el sistema operativo más popular del planeta ante la realidad de estar permanentemente conectados a una red hostil. No importa si nuestro sistema es el más seguro, es necesario estar al tanto de todas las actualizaciones y notas de seguridad si queremos confiar en que nuestra computadora responde únicamente a nuestras órdenes y que lo hace de forma confiable.

Incluso ante el mismo programador, como proféticamente lo demostró en 1984 Ken Thompson al aceptar el premio Turing (reconocido en nuestro campo como el *premio Nobel de la Ciencia de la Computación*) con el artículo *Reflexiones acerca de la confianza en la confianza*[1]; un programador siempre confía ciegamente en un conjunto de programas sobre los cuales construye (compilador, ligador, sistema operativo) y por tanto, un atacante determinado sólo tiene que *bajar lo suficiente* para plantar un troyano.

Desconfiando del DRE… y de lo demás

[8]Expertos en seguridad informática no tardaron en señalar diversas fallas elementales en el voto DRE; la principal, la confiabilidad. Si los votos *únicamente son grabados en la memoria electrónica* ¿Cómo puede asegurarse que reflejen fielmente el sentido del voto de cada individuo? O puesto de otro modo, ¿cómo podr

La respuesta no se hizo esperar: A cada voto emitido, sería impreso un comprobante o *testigo del voto*, mismo que serviría para contar los votos manualmente en caso de impugnación. Este esquema es conocido como *VVPAT* (*Voter-verified paper audit trail*, *rastro auditable en papel verificado por el votante*).

Si bien ha sido aceptado por numerosos sistemas electorales en el mundo, sigue sin ser suficiente. Como sugiere Federico Heinz[2], hay varios esquemas que podrían *reventar* una elección con este planteamiento. Por ejemplo, si las personas interesadas en sabotear una urna, tras votar, reclaman ante la mesa de autoridades indicando que la urna registró un voto contrario a lo que se le solicitó, podrían llevar a la anulación de *todos los sufragios* emitidos por dicha

urna, dado que son potencialmente ilegítimos.

Por otro lado, podría presentarse nuevamente el escenario que se dio en la ciudad de Nueva York en 2010[3]: Al calentarse las urnas electrónicas, se *emitían votos aleatorios por error*. Se estima que esto pudo haber invalidado hasta el 30% de los votos efectivos de algunas mesas.

La futilidad de los simulacros

Este 2012, el principal proyecto de implementación de voto electrónico en México fue en las elecciones locales del estado de Jalisco. Uno de los muchos puntos preocupantes de este ejercicio es que, como pruebas previas a la instalación de más de mil urnas electrónicas en dos distritos electorales y un municipio, las únicas pruebas de confiabilidad disponibles para ser analizadas públicamente son cinco simulacros.

¿Qué puede comprobarse en un simulacro? Que en el mejor de los mundos posibles y sin ninguna intencionalidad maligna, las urnas funcionen como dicen funcionar. En caso de haber algún componente malicioso en las urnas, es del total interés de quien lo haya sembrado que *no* cause ningún comportamiento inusual (para no perder su agente encubierto sin obtener la ventaja que le llevó a introducirlo). Un simulacro busca demostrar que, bajo condiciones controladas, la elección no colapsa. Lo peor del caso es que en este sentido, 3 de los 4 simulacros que habían ocurrido hasta la fecha en que este documento fue escrito, registraron fallos diversos que hacían (a menos de dos meses del proceso electoral) replantearse si se emplearían o no[4]. En el Distrito Federal, la implementación de urnas electrónicas licitadas a la misma empresa que las provee en Jalisco fue rescindida, en parte, por haberse encontrado 28 fallas[5].

¿Un simulacro exitoso aseguraría que no habrá fallas el día de la elección? ¡De ninguna manera!

Por restricciones de espacio, en este texto apenas me ha sido posible arañar algunos de los puntos más notorios del voto electrónico y de por qué, comprendiendo puntos básicos de seguridad en cómputo y estando conscientes de la gran importancia que tiene el voto dentro de un sistema democrático representativo, como el que aspiramos tener en nuestro país, resulta imposible confiar en que las urnas electrónicas resuelvan nuestros problemas de confianza, muy por el contrario.

Se ha hablado de emplear al voto electrónico para resolver otros problemas, como el del costo o la agilidad de la transmisión de resultados. Estos puntos pueden desmenuzarse y descartarse con todavía mayor facilidad que el aquí presentado.

Si este breve artículo resultó de su interés, les invito a leer el artículo publicado a fines de 2011[6], así como el abundante material que al respecto ha generado la *Fundación Vía Libre* (Argentina) [7], destacando el libro *Voto electrónico: los riesgos de una ilusión*, publicado en 2009[8].

---

[1] *Reflections on Trusting Trust*, Ken Thompson, Communications of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763

[2] [9] *Urnas electrónicas: con imprimir el voto no alcanza*, Federico Heinz, Fundación Vía Libre, septiembre de 2010; http://www.vialibre.org.ar/2010/09/12/urnas-electronicas-con-imprimir-el-voto-no-alcanza/ [10]

[3] [11] *Machine Casts Phantom Votes in the Bronx, Invalidating Real Ones: Report*, The Empire, mayo de 2012; http://www.wnyc.org/blogs/empire/2012/may/09/reports-find-machine-errors-led-uncounted-votes-2010/ [12]

[4] [13] *Pide diputada que IEPC esté listo a llevar a cabo elección tradicional*, Zaira Ramírez, El Informador, 8 de mayo de 2012; http://www.informador.com.mx/primera/2012/374801/6/pide-diputada-que-iepc-este-listo-a-llevar-a-cabo-eleccion-tradicional.htm [14]

[5] [15] *Urnas electrónicas tienen 28 fallas: IEDF*, Jonathan Villanueva, El Universal, 13 de abril del 2012; http://www.eluniversal.com.mx/ciudad/111073.html [16]

[6] [17] *Voto electrónico: ¿Quién tiene realmente la decisión?*, Construcción Colaborativa del Conocimiento (IIEc-UNAM), Gunnar Wolf, 2011; http://seminario.edusol.info/seco3/pdf/seco3_apend3.pdf

[18]

[7] [19] *Fundación Vía Libre — Voto electrónico* http://www.votoelectronico.org.ar/ [20]

[8] [21] *Voto electrónico: los riesgos de una ilusión*, Fundación Via Libre, 2009; http://www.vialibre.org.ar/wp-content/uploads/2009/03/evoto.pdf [22]

Gunnar Eyal Wolf Iszaevich [23]

numero-14 elecciones simulacro urnas electrónicas voto vulnerabilidades

Universidad Nacional Autónoma de México

Universidad Nacional Autónoma de México
Directorio

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Dirección General de Cómputo y de
Tecnologías de Información y Comunicación

SSI / UNAMCERT

SSI / UNAMCERT

[CONTACTO]

URL del envío: http://revista.seguridad.unam.mx/numero-14/m%C3%A9xico-el-voto-electr%C3%B3nico-y-el-2012

Enlaces:
[1] http://revista.seguridad.unam.mx/category/revistas/numero-14
[2] http://revista.seguridad.unam.mx/category/tipo-de-articulo/elecciones
[3] http://revista.seguridad.unam.mx/category/tipo-de-articulo/simulacro
[4] http://revista.seguridad.unam.mx/category/tipo-de-articulo/urnas-electr%C3%B3nicas
[5] http://revista.seguridad.unam.mx/category/tipo-de-articulo/voto
[6] http://revista.seguridad.unam.mx/category/tipo-de-articulo/vulnerabilidades
[7] http://twitter.com/share
[8] http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/SeguridadNum14.pdf
[9] file:///C:/Users/jlopez/Documents/Documentos%20SSI/Revista%20.Seguridad/REVISTA%20No.%2014/Art%C3%ADcul
[10] http://www.vialibre.org.ar/2010/09/12/urnas-electronicas-con-imprimir-el-voto-no-alcanza/
[11]

file:///C:/Users/jlopez/Documents/Documentos%20SSI/Revista%20.Seguridad/REVISTA%20No.%2014/Art%C3%ADcul
[12] http://www.wnyc.org/blogs/empire/2012/may/09/reports-find-machine-errors-led-uncounted-votes-2010/
[13]
file:///C:/Users/jlopez/Documents/Documentos%20SSI/Revista%20.Seguridad/REVISTA%20No.%2014/Art%C3%ADcul
[14] http://www.informador.com.mx/primera/2012/374801/6/pide-diputada-que-iepc-este-listo-a-llevar-a-cabo-eleccion-tradicional.htm
[15]
file:///C:/Users/jlopez/Documents/Documentos%20SSI/Revista%20.Seguridad/REVISTA%20No.%2014/Art%C3%ADcul
[16] http://www.eluniversal.com.mx/ciudad/111073.html
[17]
file:///C:/Users/jlopez/Documents/Documentos%20SSI/Revista%20.Seguridad/REVISTA%20No.%2014/Art%C3%ADcul
[18] http://seminario.edusol.info/seco3/pdf/seco3_apend3.pdf
[19]
file:///C:/Users/jlopez/Documents/Documentos%20SSI/Revista%20.Seguridad/REVISTA%20No.%2014/Art%C3%ADcul
[20] http://www.votoelectronico.org.ar/
[21]
file:///C:/Users/jlopez/Documents/Documentos%20SSI/Revista%20.Seguridad/REVISTA%20No.%2014/Art%C3%ADcul
[22] http://www.vialibre.org.ar/wp-content/uploads/2009/03/evoto.pdf
[23] http://revista.seguridad.unam.mx/autores/gunnar-eyal-wolf-iszaevich