Página12

El país | Sábado, 4 de julio de 2015

EXPERTOS EN INFORMATICA DESCUBRIERON "AGUJEROS DE SEGURIDAD" EN EL SISTEMA INFORMATICO CON QUE SE VOTARA MAÑANA

Con los chips de punta por la falta de control

Lo comprobaron, le advirtieron al gobierno porteño, no les hicieron caso y ahora denuncian que es muy fácil "apilar" votos con un programita y un smartphone. Recomiendan contar a mano las boletas y no confiar en los chips.

Son expertos en seguridad informática, asesoran entidades de primer nivel en el país y en el exterior, se conocen de hace tiempo. Como en los viejos tiempos, volvieron a reunirse y como en un juego hurgaron en las medidas de seguridad del sistema de voto electrónico que contrató la Ciudad de Buenos Aires y que debutará –sin experiencia previa de los electores– en la elección de mañana para elegir al nuevo jefe de Gobierno. Allí descubrieron que el sistema de recuento de votos de las máquinas que usarán los porteños puede ser adulterado a través de un celular y con un código al que ellos lograron acceder pero que, preocupados, no difundirán hasta luego de la elección. Quienes dieron a conocer este "error" en el sistema de seguridad de la empresa Vot.Ar afirman que comprobaron en la práctica que esta adulteración es posible cuando la Ciudad sacó a las calles las primeras máquinas para la capacitación y adaptación de los ciudadanos al nuevo sistema de votación. Por eso aconsejan a los presidentes de mesas y fiscales usar la vieja metodología del conteo y control manual –"calculadora en mano"– de la cantidad de votos emitidos para certificar que sea el mismo que arroje la máquina, que luego, a través de los chips de cada voto, enviarán los datos para un más rápido recuento provisorio.

Las máquinas no distinguen el número de votos real del inventado, si son hackeadas, ni permiten corregir.

"Durante semanas previas a las elecciones, un grupo de entusiastas de la seguridad informática intentamos ofrecer nuestra ayuda por diferentes medios, teniendo innumerables reuniones con responsables y políticos, todas ellas en vano", arranca el informe difundido por Internet. "Nuestro objetivo era la realización de un informe sobre los aspectos físicos, lógicos y procedimentales de seguridad que fuera totalmente independiente, y por sobre todo, no partidario. Simplemente desde la posición de un ciudadano más. Ante la falta de colaboración, nuestro último recurso fue la recolección de información pública en Internet y la utilización para realizar pruebas de los puestos públicos de capacitación", continúa.

"Este documento demuestra uno de los errores de seguridad más graves encontrados, que permiten que cualquier elector malintencionado deposite una boleta en la urna con un chip grabado para alterar el resultado del escrutinio provisorio", afirman como conclusión Alfredo Ortega, Iván Ariel Barrera Oro, Enrique Chaparro, Fernando Russ, Francisco Amato, Javier Smaldone, Juliano Rizzo, Nicolás Waisman, Sergio Demian Lerner "y gente de la Internet...".

Una experiencia que "comprobamos al menos en dos de las primeras máquinas que se utilizaron para la capacitación pública de los votantes al nuevo sistema", dijo a Ortega a Página/12. "Durante nuestra investigación descubrimos que este proceso no está correctamente implementado, y a través de un error de programación es posible grabar el chip mediante un simple smartphone de forma que contenga múltiples votos a un mismo candidato", agrega el documento. Un proceso que se puede fraguar con la utilización de un código, al que ellos lograron acceder.

La Descripción e Impacto del Ataque Multivoto, como la bautizaron, desarrolla con detalles técnicos todo el proceso informático de la máquina de voto electrónico. Allí explican que, además de la certeza de poder adulterarse la cantidad de votos –a través del acceso a un código–, el sistema no tiene los controles necesarios para evitarlo. El informe agrega allí una "demostración" de la adulteración en base a una filmación que realizaron durante el hackeo a una de las máquinas en la que se instruía a los votantes.

Primero porque ante un "ataque malintencionado" que puede agregar una cantidad de votos "extras" (no emitidos legalmente) a un

candidato o boleta, el sistema de conteo informático de la máquina no le permite diferenciar entre la cantidad real de votos emitidos y la cantidad que arroje el conteo informático adulterado.

Segundo, porque durante el control posterior que realizará el presidente de mesa con el repaso de voto por voto, con su correspondiente chip, para su verificación informática, el sistema tampoco le permite restar votos –sin volver a cero– en caso de que el total haya sido adulterado previamente. Por lo tanto –afirman–, la máquina volverá a arrojar como resultado certificado el manipulado informáticamente y es el que se retransmitirá para el recuento informático provisorio.

“Durante nuestra investigación no pudimos determinar si éste y otros errores de seguridad encontrados son intencionales o se deben a la torpeza de los programadores y falta de adecuados procesos de control de calidad del software”, agrega el documento, que tampoco evita críticas al voto electrónico: “La solución de fondo de este problema es no emplear sistemas de emisión del sufragio por medios informáticos. Estos agregan nuevas posibilidades de ataques y fraudes sin solucionar ninguno de los problemas característicos de nuestro sistema electoral que no pueda ser resuelto con la boleta única de papel”.

“Hemos intentado hacer llegar nuestra preocupación sobre la fragilidad de este sistema y alertar sobre los riesgos a diferentes autoridades sin éxito. Fracasada esta opción, nuestra responsabilidad como ciudadanos y como practicantes de la seguridad informática nos obliga a publicar esta información”, concluyen.

Un inconveniente que se puede saldar, como dijo Ortega a Página/12 y en el que insiste el propio documento, con una vieja alternativa de acceso más cotidiano: “Calculadora en mano”. La firma que desarrolló la plataforma coincide, pero avisa que difícilmente se pueda practicar el fraude porque el voto se hace a la vista de las autoridades de mesa.

© 2000-2016 www.pagina12.com.ar | República Argentina | Todos los Derechos Reservados

Sitio desarrollado con software libre GNU/Linux.