Julio 3, 2015

Ataque a sistema de voto electrónico Vot.Ar (BUE) permite sumar multiples votos con una sola boleta.

Introducción

El sistema de voto electrónico *vot.ar* escogido para las elecciones locales de la ciudad de Buenos Aires, inspeccionado por la Facultad de Ciencias Exactas y Naturales de la UBA a solicitud del Tribunal Superior de Justicia de la ciudad, **permite alterar los resultados del escrutinio en cada mesa**.

El domingo 5 de julio del 2015 se realiza por primera vez en la Ciudad de Buenos Aires una elección empleando un sistema de voto electrónico. Son muchas las polémicas que genera tanto a nivel legal como técnico en el ámbito de la seguridad informática.

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.

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.

Este documento demuestra uno de los errores de seguridad más graves encontrados, que permite que cualquier elector malintencionado deposite una boleta en la urna con un chip grabado para alterar el resultado del escrutinio provisorio.

Descripción e impacto del Ataque Multivoto

El presidente de mesa entrega a cada votante inscrito en el padrón una boleta. Esta contiene un ***tag* de identificación por radiofrecuencia (RFID)**, compuesto de un circuito integrado (“chip”) y una antena. Mediante las máquinas de Vot.Ar, el elector elige los candidatos de su preferencia, y esta selección **se graba en el chip y se imprime en la boleta**, que es luego depositada en una urna tradicional.

Al finalizar los comicios, el presidente de mesa **abre la urna y comienza el conteo** de los votos empleando la misma máquina *vot.ar* mediante otra función del programa. Para efectuar el conteo:

- Apoya la boleta en la máquina -> se contabiliza un voto.
- Apoya la próxima boleta -> se contabiliza otro voto.

Y así hasta finalizar el recuento. El software de la máquina de voto (PC corriendo sistema operativo Ubuntu 14.04) **no permite restar votos al recuento sin volver a cero**.

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.
Cuando el presidente apoye la boleta en la máquina, ocurrirá lo siguiente:

- Una boleta con chip -> **se contabilizan múltiples votos**.

Video de demostración

https://www.youtube.com/watch?v=CTOCspLn6Zk

Detalles técnicos

El pseudo-código del programa que lee y cuenta los votos es:

```
class Selection(object):
 ...

    def from_string(TAGcontent):
        datatag = parse(TAGcontent)

 ...

      candidates = []
        for e in datatag.vote:
            party_code = e["party"]
            category_code = e["category"]
            candidate = CandidateClass.get(category_code,
                                           party_code)
            candidates.append(candidate)
```

Primero se leen los datos del chip de la boleta y se almacenan en la variable *datatag*. Después se interpreta la selección y se agrega a la lista *candidatos*.

El código NUNCA verifica si hay más de un voto para el mismo candidato por elector, y tampoco limita un número máximo de votos por boleta.

La función `parse()` falla también en verificar los datos de forma alguna.

Luego, la clase "`Count()`" suma los votos. Este es el pseudo-código:

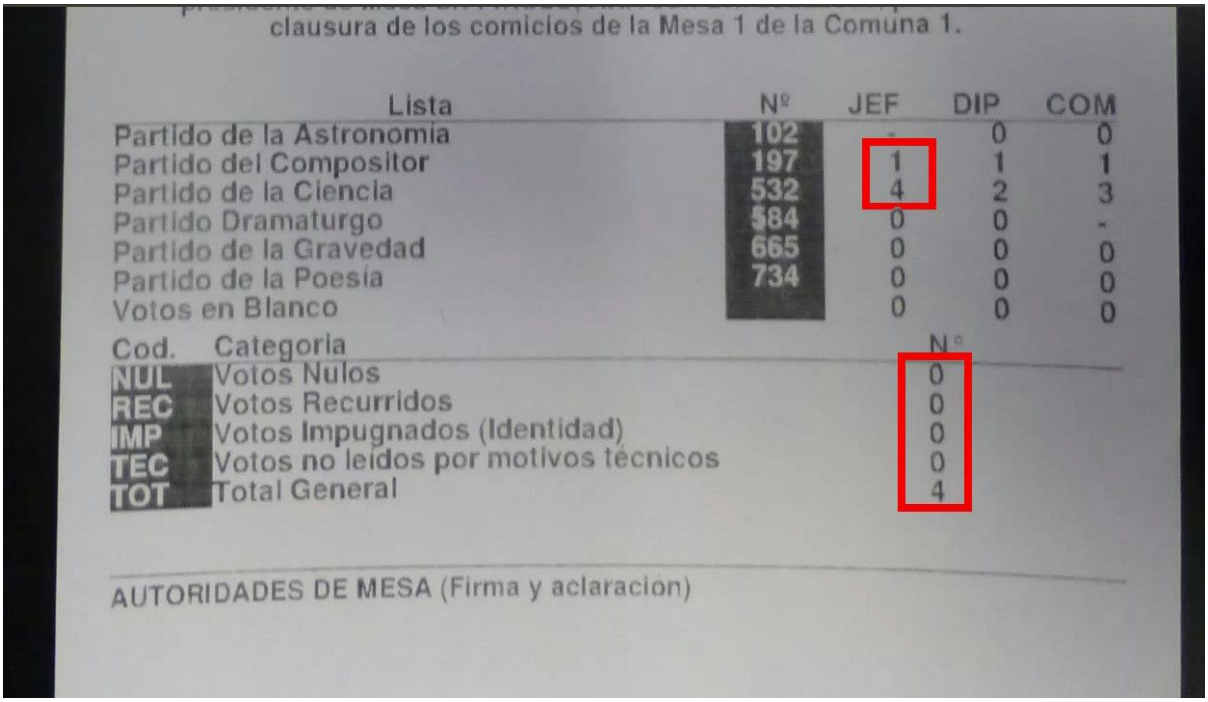
```
class Count(object):

 ...
   def add_selection(self, selection, RFIDserial=None):
        if not RFIDserial or not self.serial_exists(RFIDserial):
            for candidate in selection.candidates:
                self.results[candidate.party_code,
candidate.category_code] += 1
            if RFIDserial:
                self._RFIDserials.append(RFIDserial)
  ...
        else:
            raise RepeatedSerial()
```

Aquí la lista que contiene los múltiples votos es agregada a la variable '`results`'. Nuevamente, no hay mecanismo alguno que detecte votos repetidos.

Falla de Recuento

Este problema podría haberse subsanado en la fase de recuento de votos asegurándose de que la suma de votos coincida con la cantidad de boletas. Como puede verse en la siguiente fotografía de la impresión, esta verificación no se realiza:



clausura de los comicios de la Mesa 1 de la Comuna 1.

Lista	Nº	JEF	DIP	COM
Partido de la Astronomia	102	-	0	0
Partido del Compositor	197	1	1	1
Partido de la Ciencia	532	4	2	3
Partido Dramaturgo	584	0	0	-
Partido de la Gravedad	665	0	0	0
Partido de la Poesia	734	0	0	0
Votos en Blanco		0	0	0

Cod.	Categoria	N°
NUL	Votos Nulos	0
REC	Votos Recurridos	0
IMP	Votos Impugnados (Identidad)	0
TEC	Votos no leidos por motivos técnicos	0
TOT	Total General	4

AUTORIDADES DE MESA (Firma y aclaración)

La máquina emite acta con un total de votos a Jefe de Gobierno mayor al total general.

Prueba de concepto

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 para que autoridades de mesa y fiscales estén alerta durante el recuento.

El error detectado no es único, sino un ejemplo de un problema lógico en una de las funciones principales del sistema. Su constatación hace evidente que **los programas no fueron auditados conforme a las reglas del arte**, en particular para una aplicación que es crítica en la ejecución de un proceso fundamental de la democracia.

La información que permite reproducir este “ataque de boleta multivoto” ya se ha hecho pública por diversos medios. Como medida paliativa, no publicaremos código que facilite la creación de boletas fraudulentas hasta después de transcurrida la elección.

Estamos a disposición de las autoridades, los partidos y/o periodistas que estén interesados en comprobar la vulnerabilidad que se describe en este documento.

Solución Paliativa

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.
El sistema fue impuesto de forma apresurada, sin educación apropiada a los ciudadanos ni las autoridades y **sin una auditoría de código exhaustiva**, como claramente deja en evidencia este ejemplo de error de programación. Por otra parte, la experiencia internacional muestra que todo sistema de voto electrónico, más temprano que tarde, ha resultado vulnerable a alguna forma de ataque.

Como paliativo, recomendamos enfáticamente a los presidentes de mesa y a los fiscales realizar la contabilidad boleta por boleta haciendo énfasis en la impresión por sobre la información del chip. Es **indispensable** asegurarse de que la cantidad de boletas coincide exactamente con los votos contados por la máquina.

Con carácter más general, pero no menor importancia, recomendamos **no confiar en los resultados generados por la máquina** *vot.ar*, ya que aunque no hubiera sido manipulada maliciosamente, la aparición de este grueso error ante una inspección limitada en tiempo y medios permite inferir una programación deficiente y el probable surgimiento de otros errores críticos.

Aconsejamos desarrollar un procedimiento manual en paralelo, ejecutado por las autoridades de mesa y los fiscales del mismo modo que históricamente se ha ejecutado para las elecciones convencionales.

LLEVAR CALCULADORA PARA CONTROLAR EL ACTA

En la medida de nuestras posibilidades desarrollaremos una aplicación móvil para detectar el ataque en las boletas electrónicas.

Recomendación

Durante nuestra investigación, notamos que la forma y el estilo de la programación del sistema no parece realizada bajo los estrictos estándares que requieren aplicaciones de infraestructura crítica.

Durante nuestra investigación no pudimos determinar si este 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.

Desde el campo de la seguridad de los sistemas de información evaluamos que los riesgos que introduce el voto electrónico en términos de errores accidentales o ataques maliciosos a gran escala y fáciles de encubrir superan con holgura los beneficios reales o percibidos de la automatización de un paso crítico del sistema electoral.

Se ha generalizado la creencia que todo sistema social puede ser migrado a un sistema de computadoras, y que esto implica automáticamente una mejora en términos de agilidad y economía, sin ninguna contrapartida. Existen ciertas aplicaciones, con requerimientos críticos de seguridad informática, privacidad y usabilidad, para los cuales la tecnología actual aún no puede dar respuesta. Estos sistemas son complejos y a mayor complejidad, mayor es el riesgo de falla.

La comunidad académica y la industria aún no saben cómo hacer máquinas y sistemas seguros de este tipo. Por esta razón, la buena intención de explorar la migración tecnológica del sistema de votación debe estar englobada en un proyecto que incluya múltiples iteraciones de análisis y retroalimentación con los diversos actores de la comunidad.
Ningún avance técnico debe debilitar la democracia.

Adhieren:
Alfredo Ortega
Ivan Ariel Barrera Oro
Enrique Chaparro
Fernando Russ
Francisco Amato
Javier Smaldone
Juliano Rizzo
Nicolas Waisman
Sergio Demian Lerner

Y gente de la Internet..