Análisis de la integridad de datos en Sistemas de e-Voting

Germán Montejano [1 2]; Pablo García[2]; Silvia Bast[2]

[1]Departamento de Informática
Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
Tel.: +54-2652-424027 – Int. 251
gmonte@unsl.edu.ar – web: http://www.unsl.edu.ar

[2]Departamento de Matemática
Universidad Nacional de La Pampa
Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina
Tel.: +54-2954-425166– Int. 28
[pablogarcia, silviabast]@exactas.unlpam.edu.ar

Resumen

Las TIC cumplen un papel primordial en la sociedad actual. Su evolución ha producido cambios profundos en distintas áreas y también en la forma de relacionarse de las personas. La sociedad actual ha delegado en ellas muchas tareas fundamentales para su propio funcionamiento, dando lugar a lo que se denomina sociedad del conocimiento.
La incorporación del voto electrónico en las sociedades democráticas parece surgir como una evolución natural dentro del proceso de transformaciones sociales que se está llevando a cabo actualmente. Sin embargo, existen fuertes cuestionamientos en cuanto a su uso.
Para que la introducción de la tecnología sea exitosa, se deberá probar que los sistemas automáticos son confiables. En búsqueda de ese objetivo, se hace necesario estudiar todos los aspectos que generan dudas en cuanto a su uso, entre los cuales, la integridad de datos es de especial interés. Este trabajo se propone realizar un análisis acerca del estado del arte de los sistemas de voto electrónico focalizando en el aspecto de la integridad de los datos.

Palabras clave: ***sistemas de voto electrónico, seguridad, requerimientos, integridad de datos.***

Contexto

El presente trabajo se enmarca en el Proyecto de Investigación: "Ingeniería de Software: Aspectos de Alta sensibilidad en el ejercicio de la Profesión del Ingeniero de Software", dentro de la línea de investigación denominada “Ingeniería de Software y Defensa Cibernética” presentada en WICC 2013[1], en el ámbito de la Facultad de Ciencias Físico-Matemáticas y Naturales de la Universidad Nacional de San Luis.

Introducción

Las personas realizan en forma creciente y a diario tareas mediadas por plataformas tecnológicas. Si bien existen actividades que los usuarios no dudan en realizar a través de la tecnología, hay otras cuya informatización es más resistida, tal es el caso del voto electrónico.

Tal como se expresa en [2] *"Las tecnologías se presentan hoy como la encarnación de los valores de una sociedad democrática: la libertad, la igualdad y el intercambio"*. Sin embargo no se observa el mismo nivel de aceptación que en la mayoría de los servicios relacionados con e-gobierno.

La implementación del voto electrónico, es un tema que se ha vuelto más notorio en las dos últimas décadas y ha generado profundos debates acerca de los beneficios y de las desventajas que supone la incorporación de nuevas tecnologías en los procesos electorales.

Los requerimientos de los sistemas de voto electrónico

El voto electrónico puede definirse como un método en el cual los votos son emitidos o tabulados por medios electrónicos. Un sistema de voto electrónico es un componente de software que mapea el procedimiento de voto electrónicamente [3].

En la actualidad, en muchos países se han desarrollado experiencias de voto electrónico con distintas soluciones y tecnologías tales como: tarjetas perforadas, scanners ópticos, Direct Recording Electronic (DRE), sin embargo, en todos los casos se han presentado objeciones a los sistemas utilizados. Las discusiones que se plantean focalizan sobre las características que debe tener un sistema de voto electrónico.

Estos sistemas tienen defensores y detractores, ambos con argumentos sólidos. Sus defensores sostienen que sus ventajas son múltiples:

- La primera y más importante es la velocidad con la que se conocen los resultados. Este punto no es trivial, dado que apunta a reducir la incertidumbre que se genera entre el momento en que se da por finalizado el acto eleccionario y el de conocer los resultados oficiales. Este lapso de tiempo ha sido en muchos casos, el origen de conflictos importantes. En ocasiones, ésto ha producido sólo malos entendidos, pero en otros los conflictos han alcanzado niveles importantes. Mientras los resultados oficiales no son conocidos, la sociedad entera se encuentra en un estado de tensa espera para conocer quiénes asumirán la conducción y qué proyecto será el que se desarrolle hasta la próxima elección.
- Se suprime la posibilidad de ocurrencia de algunos vicios típicos de un sistema manual, tales como: robo de boletas, colocación al tope de todas las pilas de una boleta determinada, adulteración de actas y de telegramas donde se informan los resultados electorales, embarazo de urnas, voto cadena o soborno de las personas que cuentan los votos.
- Disminuye la cantidad de votos nulos, dado que el votante sólo podrá elegir entre alternativas válidas.
- Se reduce notablemente el número de personas afectadas al proceso de fiscalización, y como consecuencia se obtiene una mayor igualdad entre los partidos participantes, independientemente de su porte.
- Si la metodología usada es el voto electrónico por Internet, es factible que se incremente el nivel de participación de los ciudadanos, ya que aquellas personas que están imposibilitadas de asistir a la mesa de votación, podrán emitir el sufragio desde sus hogares o centro de residencia.
- Favorece el voto de migrantes.

Los detractores, en cambio, aducen las siguientes desventajas:

- Naturalmente la gente tiende a desconfiar de un esquema electrónico.
- Algunos países precursores en este tipo de avance tecnológico han abandonado este sistema.
- Aumenta la exigencia de capacitación de las personas que van a auditar el proceso.
- Aparecen problemas que no existen en el modelo manual, tales como:
    - Ataques a la base de datos, que pueden permitir que intrusos obtengan información sobre los votos y los votantes e incluso que cambien los resultados de la elección.
    - Ataques a los canales de comunicación, la respuesta para esta problemática es estrictamente criptográfica.
    - Dificultad para mantener el anonimato [4], [5] y [6] Los votos electrónicos quedan almacenados en medios magnéticos y por lo tanto es difícil garantizar que no quede alguna copia no autorizada. Personas con tiempo y recursos podrían trabajar en la decodificación y terminar relacionando a un voto con su emisor. En las votaciones manuales eso no ocurre porque los votos se queman pasado cierto lapso de tiempo.
    - Inconvenientes para garantizar la transparencia. En los sistemas electrónicos existen partes del proceso que no pueden ser fiscalizadas con facilidad.

La confianza de la sociedad sobre el sistema que se usa parece ser un punto central para lograr la aceptación del mismo. La exigencia en ese sentido es muy significativa dada la importancia de lo que se pone en juego en una elección.

Los requisitos que debe cumplir un sistema de voto electrónico coinciden en parte, con aquellos que debe verificar cualquier sistema basado en tecnología, pero además existen otros que son específicos. En [7], [8], [9] y [10] se proponen conjuntos de requerimientos que deben respetar los mencionados sistemas. Los mismos pueden resumirse:

- *Secreto:* esto implica que el voto debe ser conocido únicamente por quién lo emitió. Por lo tanto debe eliminarse la posibilidad de relacionar a los votantes y sus preferencias indefinidamente. Debe ser imposible además, aún para el elector probar a una tercera parte por quién votó.
- *Autenticación del votante*: sólo las personas que figuran en el padrón de electores pueden emitir un voto. Se torna necesario entonces, verificar que el emisor sea un votante acreditado para luego registrar su sufragio
- *Verificabilidad*: debe ser posible verificar los siguientes aspectos: que los votos se contabilicen tal como se emitieron, que sólo los votos de electores habilitados se incluyan en el recuento final, que cada votante emita un único voto y que el resultado del recuento final coincida con la voluntad de los votantes.
- *Simplicidad:* el sistema debe ser lo suficientemente sencillo e intuitivo como para que personas que no son expertas ni están en contacto cercano con la tecnología, puedan usarlo. Debe evitar confusiones a los usuarios, soportar la accesibilidad de personas con capacidades especiales y las diferencias lingüísticas de los votantes.
- *Costo*: la adquisición, mantenimiento y operación del sistema debe poder realizarse a un costo razonable.

- *Auditabilidad:* El proceso electoral debe poder ser auditado en cualquiera de las etapas, fundamentalmente en la obtención de resultados.
- *Inviolabilidad*: debe impedirse el cómputo parcial de la elección antes de que termine el proceso eleccionario, dado que esto podría influenciar al resto de los votantes y afectar el resultado final.
- *Seguridad*: debe ser imposible, tanto para una persona interna a la organización de las elecciones como para alguien externo manipular los resultados de las elecciones.
- *No coerción:* se debe garantizar que los votantes no pasen por alguna de las siguientes situaciones: verse forzados a emitir votos inválidos, abstenerse bajo presión o que otra persona tome su lugar.
- *Robustez*: ninguna entidad debe interrumpir el proceso de voto, el sistema debe ser capaz de detectar acciones deshonestas y completar el proceso normalmente.
- *Escalabilidad*: el esquema debe poder extenderse fácilmente para satisfacer requerimientos de computación, comunicación y almacenamiento de elecciones a gran escala.

Entre los requerimientos mencionados, existen algunos que pueden satisfacerse de forma sencilla, pero otros presentan mayor nivel de dificultad. Inclusive hay algunos que parecen tener algunas contradicciones entre ellos, tal es el caso de verificabilidad, que requiere que se vinculen los electores a los votos y por lo tanto presenta una clara contradicción con la característica de Secreto. Debido a lo expuesto anteriormente es que algunos autores concluyen, que muchos de los sistemas de voto electrónico existentes no pueden satisfacer todos los requerimientos exigibles.

Líneas de Investigación, Desarrollo e Innovación

Las líneas de investigación que se siguen son:

- Abstracción de los criterios en los que se basará la investigación a través del análisis de las características y requerimientos de los sistemas de voto electrónico.
- Búsqueda y evaluación de sistemas de voto electrónico existentes, tomando como base los criterios mencionados en el punto anterior.
- Elaboración de conclusiones en base al análisis previo.
- En base a las conclusiones obtenidas, presentar alternativas tendientes a garantizar la integridad de los datos.

Resultados y Objetivos

Para conocer el estado del arte en cuanto a la integridad de datos en los sistemas de voto electrónico, se investigó sobre las características y requerimientos que los mencionados sistemas deben poseer, posteriormente se efectuó una selección de los requerimientos que están vinculados más cercanamente con el concepto de integridad de datos y finalmente se realizó la búsqueda de sistemas de voto electrónico existentes.

Actualmente se encuentra en desarrollo la etapa de búsqueda y evaluación de sistemas de voto electrónico existentes a la luz de los requerimientos seleccionados previamente.

Se espera realizar una comparación de algunos sistemas existentes, para poder identificar debilidades y fortalezas y proponer estrategias que permitan obtener mejoras en lo relativo a integridad de datos.

Formación de Recursos Humanos

En el marco del presente proyecto se presentan los siguientes puntos relacionados con la formación de recursos humanos:

- Pablo García realizó una estadía de un año en la Universidad Federal de Minas Geráis (UFMG), aprobando seminarios de posgrado y trabajando en el grupo "Criptografía Teórica y Aplicada", dirigido por Jeroen van de Graaf, PhD.
- Pablo García defendió su tesis para obtener el grado de Magister en Ingeniería de Software de la Universidad Nacional de San Luis, bajo la dirección de Jeroen van de Graaf, PhD (UFMG) y Dr. Germán Montejano (UNSL). La tesis se tituló: "Optimización de un Esquema Dining Cryptographers Asíncrono" y recibió la calificación de sobresaliente.
- Silvia Bast está desarrollando su tesis para obtener el grado de "Especialista en Ingeniería de Software". Su plan de trabajo fue aprobado y se planea su defensa para junio de 2014. La tesis se titula: "Sistemas de E-Voting: Integridad de Datos" y está dirigida por el Dr. Germán Montejano (UNSL) y el Magister Pablo García (UNLPam).
- Pablo García está desarrollando su tesis para obtener el grado de "Especialista en Ingeniería de Software". Su plan de trabajo fue aprobado y se planea su defensa para junio de 2014. La tesis se titula: "Anonimato en sistemas de Voto Electrónico" y es dirigida por Jeroen van de Graaf, PhD (UFMG) y Dr. Germán Montejano (UNSL).

Referencias

[1] **Uzal R., van de Graaf, J., Montejano G.,Riesco D., García P**.: "Inicio de la Línea de Investigación: Ingeniería de Software y Defensa Cibernética". Memorias del XV WICC. Ps. 769 - 773. ISBN: 9789872817961. 18-19/04/2013.

[2] **Busaniche, B., Heinz, F. [et alt.]** "Voto Electrónico: los riesgos de una ilusión" 1ra ed. Córdoba: Fundación Vía Libre ISBN 978-987-22486-5-9
Edición a cargo de Beatriz Busaniche y Federico Heinz, 2008

[3] **Odrisek, B.**: "E-Voting Security Study"-Communications-Electronics Security Group, X/8833/4600/6/21, (Copyright The Crown) Issue 1.2 31 United Kingdom, 2002.

[4] **van de Graaf, J., Montejano G., García P.**: "Optimización de un esquema "Ocuppancy Problem" orientado a E – Voting". Memorias de XV WICC. Ps. 749-753. ISBN:9789872817961. 18-19/04/ 2013.

[5] **van de Graaf, J., Montejano G., G García P.**: "Manejo de Colisiones en un Protocolo Non Interactive Dining Cryptographers". Anales de las 42° JAIIO, (ISSN: 1850-2776). Workshop de Seguridad Informática (WSegI 2013, ISSN: 2313-9110). Ps. 29 a 43. 09/2013.

[6] **van de Graaf, J., Montejano G., García P.**: "Optimización de un Protocolo Non-Interactive Dining Cryptographers". Congreso Nacional de Ingeniería Informática/Sistemas de Información. CoNaIISI-2013.21-22 /11/2013. Córdoba, Argentina.

[7] **Epstein, J.** "Electronic Voting", Cyber Defense Agency LLC.

[8] **Kazi Md. Alam Rokibul; Tamura, Shinsuke**, Electronic Voting - Scopes and Limitations IEEE/OSA/IAPR International Conference on Infonnatics, Electronics & Vision

[9] **Prince, A.:** Consideraciones, aportes y experiencias para el Voto electrónico en Argentina. 2005.

[10] **van de Graaf, J., Henrich C., Müller-Quade, J**.: "Requirements for secure voting". Notas de Trabajo. 2011.