Avances sobre la Especificación Integral del Sistema OTP-Vote Orientada a su Implementación

Silvia Bast[1] Germán Montejano[2] MarioBerón[2]

[1]Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad Nacional de La Pampa
Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina
Tel.: +54-2954-425166– Int. 28
silviabast@exactas.unlpam.edu.ar – web: http://exactas.unlpam.edu.ar/

[2]Departamento de Informática
Facultad de Ciencias Físico Matemáticas y Naturales
Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
Tel.: +54-2652-424027 – Int. 251
[gmonte, mberon]@unsl.edu.ar – web: http://www.unsl.edu.ar

RESUMEN

El sistema electoral que rige en Argentina tiene sus bases en la Ley Saénz Peña de 1912, que establece que el voto debe ser: universal, secreto y obligatorio. Si bien este sistema manual, que se usa actualmente en la mayoría de los distritos del país, funciona de manera aceptable, es también permeable a algunos vicios. Por otro lado, la incorporación del voto electrónico presenta grandes discusiones debido, especialmente, a falta de confianza del electorado. El principal desafío de este proyecto es aportar propuestas para la construcción de un sistema de votación electrónica robusto y confiable. El trabajo de investigación tiene sus orígenes en el modelo inicial de datos de un sistema de voto electrónico denominado OTP-Vote. Con vistas a lograr su implementación, se deben especificar en profundidad un conjunto de características que se mencionan como supuestos en el modelo inicial. En este artículo se describen los aspectos en los que se ha avanzado con el objetivo de obtener un sistema sólido y seguro.

Palabras clave: Sistemas de Voto Electrónico, Anonimato, Transparencia, Auditoría, One Time Pad, Verificabilidad End to End.

CONTEXTO

Este trabajo se enmarca en el Proyecto de Investigación denominado: "Especificación Integral del Sistema OTP-Vote Orientada a su Implementación", que se desarrolla en el ámbito de la Facultad de Ciencias Exactas y Naturales (FCEyN) de la Universidad Nacional de La Pampa (UNLPam), Resolución N° 55/22 del Consejo Directivo FCEyN - UNLPam y es dirigido por el Doctor Germán Antonio Montejano (Universidad Nacional de San Luis) y por el Doctor Mario Berón (Universidad Nacional de San Luis) y es la continuación de la línea de investigación “Desarrollo de un Modelo de Voto Electrónico basado en Criptografía One Time Pad” del proyecto "Aspectos de Seguridad en Proyectos de Software, Resolución N° 488/14 del Consejo Directivo de FCEyN - UNLPam.

1. INTRODUCCIÓN

El sistema electoral argentino ha presentado algunas mejoras desde sus inicios, una de las más importantes es la aplicación de la Ley Saénz Peña o Ley Nacional de Elecciones N° 8.871, de 1912 que estableció las características del voto que perduran hasta hoy: universal, secreto y obligatorio.

El sistema manual que se usa en la actualidad funciona de manera aceptable, aunque es permeable a algunos vicios tales como: robo de boletas, colocación al tope de todas las pilas de una boleta determinada, adulteración de actas y telegramas, embarazo de urnas, voto cadena, soborno a personas que realizan el conteo de los votos, entre otras. Además, en algunos países la cantidad de candidatos para cada cargo y también el gran número de votantes dificultan y lentifican el proceso de conteo para la publicación final de los resultados.

Ante este diagnóstico, la incorporación de los sistemas de voto electrónico, parece ser el paso natural en el proceso de transformaciones sociales que se produce día a día. Sin embargo, existen fuertes cuestionamientos del electorado a este tipo de sistemas, que radican especialmente en la falta de trasparencia.

Las personas compran en línea, realizan operaciones bancarias online, se reúnen virtualmente, enseñan y evalúan a los estudiantes de manera virtual, pero no se sienten suficientemente confiados para hacer uso de un sistema de voto electrónico.

Estudiando las razones por las que la ciudadanía actúa de forma diferente ante el uso de los sistemas, surge que, los ciudadanos realizan con confianza operaciones en las que de alguna manera queda un comprobante o registro que vincula la actividad realizada con la identificación de quién la realizó. Por ejemplo, una operación bancaria con el documento de identidad de la persona o la clave única de identificación bancaria, o un legajo de estudiante con un examen. En cuanto a los sistemas de voto electrónico, los ciudadanos esperan que la identidad solo quede registrada para verificar la participación en los comicios, pero que de ninguna manera pueda ser asociada al voto. Otra característica propia de estos sistemas, es que los electores una vez que emitieron su voto, ya no cuentan con el comprobante para hacer el reclamo porque el voto queda en la sede de votación. Estas situaciones no afectan únicamente a los sistemas de votación electrónica sino a todos los sistemas electorales en general.

Desde el equipo de trabajo que lleva adelante esta investigación, se asume que:

- Los sistemas de voto electrónico se clasifican dentro de la categoría de "críticos".
- El sistema manual que se usa actualmente, tal como viene funcionando ofrece prestaciones aceptables.
- Resulta un desafío generar un modelo que permita el desarrollo de un sistema robusto y confiable.

Sistemas de Voto Electrónico

Según McGaley and Gibson [1] los sistemas de voto electrónico son "cualquier forma de recolección de votos que implique el uso de dispositivos electrónicos (usualmente computadoras)". Los requisitos que deben cumplir estos sistemas son expresados por importantes autores como Epstein [2], Kazi, Alam y Tamura [3], Prince [4], van de Graaf, Henrich y Müller-Quade [5], Hao y Ryan [6], Rivest [7], Ryan, Schneider y Teague [8], Rabin y Rivest [9] y Awad y Leiss [10].

Teniendo en cuenta que uno de los principales cuestionamiento hacia estos sistemas es la falta de transparencia y confiablidad, resulta de suma importancia que cuenten con la característica de verificabilidad extremo a extremo o verificabilidad end to end (VE2E). Esta característica permite que los electores puedan verificar que sus votos se emitieron y se contaron correctamente. Chaum [11], Ryan y Bryans [12], Chaum, Ryan y Schneider [13], Fisher, Carback, y Sherman [14], Adida y Rivest [15] y Benaloh et al [16] presentan propuestas para aportar verificabilidad a los sistemas de voto electrónico.

El Modelo OTP-Vote

En [17] se presentan las bases del modelo teórico OTP-Vote, que consiste de tres etapas, tal como se muestra en la Figura 1.

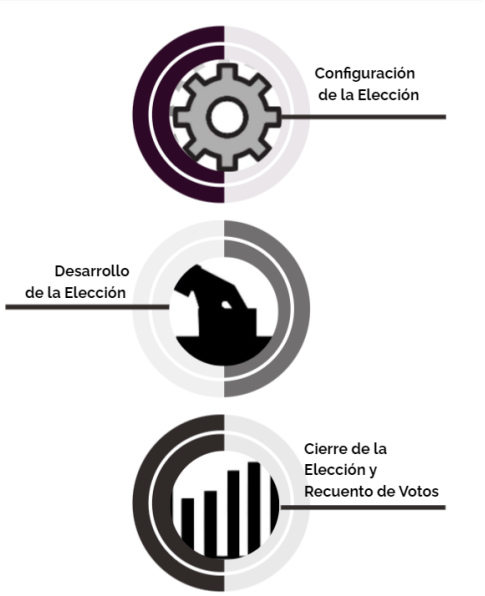

Figura 1. Etapas del Proceso Eleccionario en OTP- Vote

El modelo asegura:

- Anonimato incondicional
- Seguridad computacional que puede llevarse a cualquier nivel exigible durante el proceso eleccionario.

Para alcanzar estos objetivos usa:

- Claves One Time Pad (OTP) que cumplen con la característica de Secreto Perfecto de Shannon [18].
- El esquema de almacenamiento denominado Múltiples Canales Datos único (MCDU) y sus fórmulas propuestas para alcanzar dimensiones de los datos con comportamiento óptimo [19], [20], [21] y [22].
- La operación lógica XOR,
- La redundancia apropiada [23] en el almacenamiento de los datos.

El modelo teórico presentado supone, para cada una de las etapas mencionadas, el cumplimiento de condiciones de seguridad que resultan imprescindibles para alcanzar el normal funcionamiento del sistema.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

El modelo inicial debe ser refinado para lograr un sistema robusto e implementable. Este trabajo de refinamiento inicia con el análisis profundo de cada una de las etapas, para detectar cuáles son los aspectos críticos que deben mejorarse o especificarse, para posteriormente avanzar en propuestas superadoras que aporten soluciones a cada uno de ellos.

Será necesario profundizar en:

- La identificación y clasificación de los datos que deben permanecer inalterables durante el proceso y de aquellos que deben modificarse de forma controlada. Además, debe realizarse la búsqueda de mecanismos que permitan controlar los accesos de acuerdo a sus características.
- Propuestas de optimización de la configuración de las tuplas que almacenan los datos de los votos y los atributos de control.
- Especificación y validación de una propuesta de generación automática de tablas relacionales a partir de los datos del sistema.
- Análisis de la información que permita ofrecer transparencia al proceso a la vista de terceros, y especificación, validación y desarrollo de propuestas de auditoría.
- Especificación y validación de una propuesta de verificabilidad End to End.

3. RESULTADOS Y OBJETIVOS

Los avances de la investigación son:

- Se ha continuado y profundizado el trabajo de análisis de mecanismos que permitan realizar el acceso controlado

a los datos de acuerdo a su nivel de criticidad.

- Se ha desarrollado una propuesta de configuración de las tuplas y los atributos de control haciendo especial énfasis en la seguridad de los datos de los votos.
- Se ha trabajado en la revisión sistemática de literatura en relación a VE2E.
- Se ha desarrollado y presentado una propuesta inicial de VE2E para el sistema OTP – Vote.
- Se comenzó a trabajar en la propuesta de generación automática de tablas de datos relacionales a partir de los datos obtenidos en la etapa de configuración de la elección.

Como trabajos futuros debe avanzarse en:

- Refinamiento de protocolos antifraude que deben usarse durante todo el proceso.
- Análisis y selección de un método criptográfico que asegure la transmisión de datos entre estaciones y servidor.
- Propuestas de auditoría.
- Evaluación y mejora de los avances ya realizados sobre el modelo original.

4. FORMACIÓN DE RECURSOS HUMANOS

En cuanto a la formación de recursos humanos, Silvia Bast está avanzando en el desarrollo de la tesis denominada "Especificación Integral del Modelo OTP-Vote orientada a su impementación" para alcanzar el grado de Doctora en Ingeniería Informática en la Universidad Nacional de San Luis. Resolución de Inscripción y Aprobación de Plan de Tesis 408/21 Decanato. FCFMyN – Universidad Nacional de San Luis.

5. BIBLIOGRAFÍA

[1] M. McGaley, J. Gibson, "A Critical Analysis of the Council of Europe Recommendations on E-Voting", Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop, USENIX Association.

[2] J. Epstein, "Electronic Voting" in Computer, vol. 40, no. 8, pp. 92-95, Aug 2007. doi: 10.1109/MC.2007.271.

[3] K. M. Rokibul Alam and S. Tamura, "Electronic voting - Scopes and limitations", International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, pp. 525-529, . 2012. doi: 10.1109/ICIEV.2012.6317324.

[4] A. Prince, "Consideraciones, aportes y experiencias para el Voto electrónico en Argentina", Editorial Dunken, 2006.

[5] J.van de Graaf, C. Henrich, J. Müller-Quade, "Requirements for secure voting", Work Notes 2011.

[6] F. Hao, P. Ryan, "Real -World Electronic Voting. Design, Analysis and Deployment". CRC Press. ISBN-13: 978- 1498714693. ISBN-10: 1498714692. 2017.

[7] R. Rivest, "On the notion of 'software independence' in voting systems". Philosophical Transactions of the Royal Society A, 366(1881):3759–3767. 2008.

[8] P. Ryan, S. Schneider, V. Teague, "End-to-End Verifiability in Voting Systems, from Theory to Practice". Voting Systems, from Theory to Practice. IEEE Security & Privacy, 13(3):59–62, 2015.

[9] M. Rabin, R. Rivest, "Efficient End to End Verifiable Electronic Voting Employing Split Value Representations" Bregenz, Austria.

Proceedings of EVOTE 2014. ISBN 978-9949-23-688-6. 2014.

[10] M. Awad, E. Leiss, “End-to-End Cryptography: Spreading Democracy”. International Journal of Applied Engineering Research. Volume 11, Issue 11. Ps. 7391-7394. 2016.

[11] D. Chaum, “Secret-ballot receipts: True voter-verifiable elections“IEEE security & privacy, IEEE, 2004, 2, 38-47

[12] P. Ryan, J. Bryans. "A simplified version of the Chaum voting scheme." School of Computing Science Technical Report Series. 2004.

[13] D. Chaum, P. Ryan, and S. Schneider. "A practical voter-verifiable election scheme." European Symposium on Research in Computer Security. Springer, Berlin, Heidelberg, 2005

[14]K. Fisher, R. Carback, and A. Sherman. "Punchscan: Introduction and system definition of a high-integrity election system." Proceedings of Workshop on Trustworthy Elections. 2006.

[15] B. Adida, and R. Rivest. "Scratch & vote: self-contained paper-based cryptographic voting." Proceedings of the 5th ACM workshop on Privacy in electronic society. 2006.

[16] J. Benaloh, R. Rivest, P. Ryan, P. Stark,V.Teague, & P. Vora,(2015). End-to-end verifiability. arXiv preprint arXiv:1504.03778.

[17] S. Bast, “Confidencialidad e Integridad de Datos en Sistemas de E-Voting – Un Modelo para la Implementación Segura de un sistema de Voto Presencial”, Editorial Académica
Española. ISBN 978-3-639-53793-2. 2017.

[18] C. E. Shannon, "Communication theory of secrecy systems," in The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x..

[19] P. García, “Una Optimización para el Protocolo Non Interactive Dining Cryptographers” - Editorial Académica Española (https://www.eae-publishing.com/ - ISBN-13: 978-3-639-85270-7. ISBN-10: 3639852702. EAN: 9783639852707 – 2017.

[20] J. van de Graaf, G. Montejano, P. García, “Manejo de Colisiones en un Protocolo Non Interactive Dining Cryptographers”. Anales de las 42° Jornadas Argentinas de Informática e Investigación Operativa (JAIIO, ISSN: 1850-2776). Workshop de Seguridad Informática (WSegI 2013, ISSN: 2313-9110). Páginas 29 a 43. 2013 Disponible en: http://42jaiio.sadio.org.ar/proceedings/simposios/Trabajos/WSegI/03.pdf.

[21] García P., van de Graaf J., Montejano G., Bast S., Testa O.: “Implementación de Canales Paralelos en un Protocolo Non Interactive Dining Cryptographers”. 43° Jornadas Argentinas de Informática e Investigación Operativa (JAIIO 2014), Workshop de Seguridad Informática (WSegI 2014). http://sedici.unlp.edu.ar/handle/10915/42066. 2014.

[22] P. García, J. van de Graaf, A. Hevia, A. Viola, “Beating the Birthday Paradox in Dining Cryptographers Networks”. En “Progress in Cryptology – Latincrypt 2014”. Springer International Publishing. ISSN: 0302-9743. ISSN (electronic): 1611-3349. ISBN: 978-3-319-16294-2. ISBN (eBook): 978-3-319-16295-9. Ps. 179 – 198. Octubre, 2014.

[23] P. García, G. Montejano, S. Bast, E. Fritz, "Codificación de Sufragios con Detección de Colisiones en NIDC con Canales Paralelos de Slots” Congreso Nacional de Ingeniería en Informática / Sistemas de Información. CoNaIISI 2016.