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

La incorporación del voto electrónico en las sociedades democráticas presenta grandes controversias y discusiones entre los ciudadanos. La mayor resistencia para su implementación pasa por la desconfianza de la sociedad en tales sistemas, debido a las experiencias poco exitosas con las que los usuarios han tenido contacto en diversos lugares en elecciones recientes. Resulta claro que el problema de fondo radica en la confianza de la sociedad sobre el sistema que se usa, por lo que construir sistemas seguros y demostrar la solidez de los mismos, es el principal desafío de investigación de este proyecto.

En 2016 se presentó el modelo inicial de datos de un sistema de voto electrónico denominado OTP-Vote que asegura anonimato incondicional y seguridad computacional que puede llevarse a cualquier nivel exigible. El trabajo expone un modelado básico de los datos de los votos. Para lograr la implementación efectiva del sistema se torna necesario especificar un conjunto de aspectos de gran importancia que quedaron planteados como supuestos en el modelo inicial y que deben aportar las condiciones de seguridad para lograr un sistema de voto electrónico implementable y robusto. Se presentan a continuación los avances realizados en pos de la especificación integral del sistema.

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

CONTEXTO

El presente trabajo tiene sus orígenes en una de las líneas de investigación del proyecto "Aspectos de Seguridad en Proyectos de Software", que avanza en el desarrollo de un modelo de voto electrónico basado en criptografía one time pad. (Resolución N° 488/14 del Consejo Directivo de la Facultad de Ciencias Exactas y Naturales –FCEyN- de la Universidad Nacional de La Pampa - UNLPam).

Del mencionado proyecto surgió una tesis de maestría que presentó las bases del sistema OTP-Vote. Tomando como insumo ese trabajo, se sigue profundizando actualmente sobre la temática desarrollando una tesis doctoral

denominada “Especificación Integral del Sistema OTP-Vote Orientada a su Implementación”, en la Universidad Nacional de San Luis, avalada por Resolución 408/21 de inscripción y Aprobación de Plan de Tesis 408/21 Decanato. Facultad de Ciencias Físico Matemáticas y Naturales -FCFMyN- Universidad Nacional de San Luis - UNSL.

1. INTRODUCCIÓN

Debido a las discusiones y controversias que generan los sistemas de voto electrónico en cuanto a seguridad y transparencia, representan un desafío a los efectos de la investigación. Se torna necesario entonces analizar y evaluar las condiciones de seguridad que deben cumplir y también las soluciones que diferentes autores han propuesto hasta el momento, para intentar generar un modelo teórico que permita luego el desarrollo de un sistema robusto y confiable.

En la tesis de maestría denominada “Optimización de la Integridad de Datos en Sistemas de E-Voting”, defendida en 2016 en la Universidad Nacional de San Luis, se presentaron las bases de un modelo teórico de un sistema de voto electrónico denominado OTP-Vote. En ese trabajo se expone un modelado básico inicial de los datos de los votos, que debe ser refinado, estableciendo precisiones acerca de un conjunto de aspectos, con el fin de lograr una futura implementación.

El refinamiento propuesto apunta a otorgar mayor seguridad a través de:

- Uso de atributos de control y de encriptación, variaciones en cuanto a los datos almacenados de los votos y profundización de las posibilidades de recuperación de los mismos.
- Análisis y refinamiento de protocolos antifraude.
- Análisis y selección de un método criptográfico que asegure la transmisión de datos entre estaciones y servidor.
- Diseño de un modelo para la automatización del proceso de configuración de parámetros y generación de tablas relacionales del sistema de e-voting.
- La información intermedia que puede ser expuesta a los auditores para su control.
- Verificabilidad End to End.

Sistemas de Voto Electrónico

Un sistema de voto electrónico “es un componente de software que mapea electrónicamente el procedimiento de votación” [1].

Importantes autores como Epstein [2], Kazi, Alam y Tamura [3], Prince [4] y van de Graaf, Henrich y Müller-Quade [5], Hao, Ryan [6], Rivest [7], Ryan, Schneide y, Teague [8], Rabin y Rivest [9] y Awad y Leiss [10], expresan detalladamente los requisitos y características de estos sistemas.

El Modelo OTP-Vote

El modelo propuesto en [11] hace uso de i) claves One Time Pad (OTP) que cumplen con la característica de Secreto Perfecto de Shannon [12] (lo que significa que aún un adversario con potencia de cómputo infinita no puede deducir el texto plano a partir del texto cifrado), ii) el squema de almacenamiento denominado Múltiples Canales Datos único (MCDU) y sus fórmulas propuestas para alcanzar dimensiones con comportamiento óptimo [13], [14], [15] y [16] iii) la operación XOR [17], y iv) la redundancia apropiada [18] para el almacenamiento de los datos para asegurar:

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

El proceso de OTP-Vote consiste de tres grandes etapas como puede observarse en la figura 1.

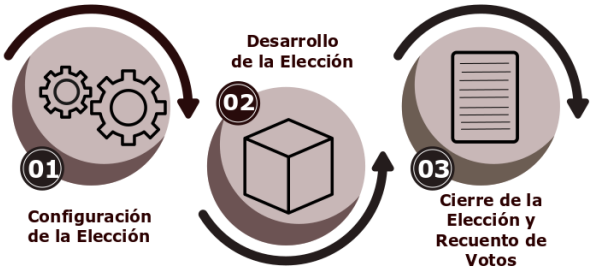

Figura 1. Etapas del Proceso eleccionario

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

Para avanzar en la investigación es necesario realizar un análisis profundo de los aspectos del modelo que requieren de condiciones óptimas de seguridad (comunicación entre usuario-sistema y sistema-servidor de datos).

Una vez identificados los aspectos a mejorar, se realizará una revisión sistemática de aportes de otros autores, para posteriormente trabajar sobre la especificación y validación de propuestas que aporten soluciones en tal sentido.

Será necesario realizar un trabajo minucioso sobre:

- Identificación de los datos que deben permanecer inalterables durante el proceso y los que deben modificarse de forma controlada, para asegurar tales condiciones.
- Análisis de la semántica de las tuplas y especificación propuestas de optimización de configuración que incluyan información 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 intermedia necesaria para dar 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

El objetivo de este proyecto es ampliar y refinar la formalización de la especificación del modelo de datos OTP-Vote publicado en 2016, en cuanto a las condiciones de seguridad antifraude para lograr un sistema de voto electrónico robusto, de inmediata y fácil implementación que permita auditorías de control y verificabilidad en todas las etapas de su uso.

Los avances en la investigación están dados por:

- Análisis de los aspectos de seguridad que involucran la comunicación del sistema con el usuario y con el servidor de datos:

i) Variaciones en la configuración de los datos en cada proceso eleccionario.

ii) Uso de atributos de control y de encriptación.

iii) Propuesta inicial de Verificabilidad End to End.

- Revisión sistemática acerca de propuestas ya existentes generadas por otros autores en relación con los aspectos analizados en i), ii) y iii).

Como trabajo futuro, tomando como base los avances ya realizados y la revisión de propuestas ya existentes debe focalizarse en los siguientes aspectos:

- Refinamiento de protocolos antifraude en todas las etapas del modelo.
- Análisis y selección de un método criptográfico que asegure la transmisión de datos entre estaciones y servidor.
- Análisis de la información intermedia que puede ser expuesta a los auditores para su control en las etapas del proceso electoral, sin comprometer el anonimato del votante.
- Elaboración de una propuesta superadora de verificabilidad End to End.
- Evaluación y profundización de los avances ya realizados sobre el modelo original.

4. FORMACIÓN DE RECURSOS HUMANOS

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

5. BIBLIOGRAFÍA

[1] B. Ondrisek, B. "E-voting system security optimization". 42nd Hawaii International Conference on System Sciences (pp. 1-8). IEEE. 2009.

[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] 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.

[12] 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..

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] M. Murdocca, V. Heuring, “Principles of Computer Architecture. Appendix A: Digital Logic”. Editor: Addison Wesley; Edición: US ed (29 de noviembre de 1999) Idioma: Inglés - ISBN-10: 0201436647 - ISBN-13: 978-0201436648

[18] 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.