Avances en Aspectos de Seguridad Aplicados a Sistemas de Voto Electrónico

Pablo García[1] Silvia Bast[1] Germán Montejano[2] Martín Lobos[1]

[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
[pablogarcia, silviabast]@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@unsl.edu.ar – web: http://www.unsl.edu.ar

RESUMEN

El debate sobre las fortalezas y debilidades del voto electrónico se encuentra en un momento de fuerte polémica, no solamente en la sociedad en general, sino también en el ámbito académico. Las argumentaciones a favor y en contra de su aplicación son muy diversas.

Los que opinan a favor, se basan en la velocidad con la que se conocen los resultados y en la (supuesta) exactitud del proceso. Los que se oponen, afirman que resulta imposible asegurar la transparencia de los sistemas de voto electrónico.

La postura asumida por este equipo de investigación, es que se trata de un sistema de seguridad crítica, y que la confianza del electorado es de máxima importancia para lograr su aceptación, tal como afirman McGaley y Gibson en [1]: "Un sistema de votación es tan bueno como el público cree que es". Este grupo de trabajo percibe estos sistemas como objetos de investigación, por lo tanto, está dedicado al análisis y evaluación de las condiciones de seguridad que deben cumplir y también al estudio de las soluciones que diferentes autores han propuesto hasta el momento, para intentar generar un modelo que facilite el desarrollo de un sistema robusto y confiable.

Se siguen, en forma paralela, dos líneas de trabajo que representan esquemas diferentes que pueden aplicarse a los sistemas de voto electrónico:

a. Basado en criptografía homomórfica.
b. Basado en criptografía One Time Pad.

En este trabajo se exponen los avances que se llevaron a cabo para cada una de las mencionadas líneas.

Palabras clave: Sistemas de Voto Electrónico, Anonimato, Transparencia, Criptografía Homomórfica, One Time Pad, Verificabilidad E2E, Prueba Física.

CONTEXTO

El presente trabajo pertenece al ámbito del Proyecto de Investigación: "Aspectos de Seguridad en Proyectos de Software", que se desarrolla en la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa (Resolución N° 488/14 del Consejo Directivo de la Facultad de Ciencias Exactas y Naturales) y es dirigido por el Doctor Germán Antonio Montejano (Universidad Nacional de San Luis) y codirigido por el Magister Pablo Marcelo García (FCEyN - UNLPam) e incluye a la Magister Silvia

Gabriela Bast, al Magister Daniel Vidoret, al Analista Programador Adrián García y al Programador Superior Claudio Ponzio como investigadores.

Surge desde la línea de Investigación "Ingeniería de Software y Defensa Cibernética", presentada en [2], que a su vez se enmarca en el Proyecto "Ingeniería de Software: Aspectos de alta sensibilidad en el ejercicio de la Profesión de Ingeniero de Software" de la Facultad de Ciencias Físico - Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL) (http://www.sel.unsl.edu.ar/pro/proyec/2012/index.html) y que incluye acciones de cooperación con la Universidad Federal de Minas Geráis (UFMG, Brasil).

1. INTRODUCCIÓN

a. Modelo Basado en Criptografía Homomórfica

La criptografía homomórfica presenta una característica muy conveniente a los efectos de implementar sistemas de voto electrónico: permite realizar operaciones sobre los datos cifrados directamente, sin necesidad de descifrarlos ni de conocer ninguna clave. Ese atributo le otorga un gran atractivo a su aplicación práctica.

Los primeros modelos de este estilo se originan a fines de los ´70. Ellos se denominan parcialmente homomórficos, porque sólo permiten un tipo de operación sobre los datos cifrados (suma o multiplicación). Son ejemplos de este tipo El Gamal [3], Benaloh [4] y Paillier [5].

A partir de [6] se produce un avance decisivo en la materia, porque se presenta el primer esquema homomórfico completo, es decir que soporta operaciones de adición y producto sobre datos cifrados.

El modelo a implementar, además de seleccionar el esquema criptográfico apropiado, deberá cumplir con una serie de requisitos que se exigen actualmente a los sistemas de votación electrónica:

- Evidencia física que garantice la transparencia del proceso [7].
- Utilización de métodos criptográficos cuya seguridad incluya formalidad matemática, tanto en lo referente al anonimato del votante como a la transparencia de los resultados de los comicios.
- Aplicación del concepto de independencia del software [8].
- Definición de un modelo concreto para la aplicación de verificabilidad "End to End" (E2E) [9].
- Aplicación de técnicas que eviten que un votante pueda demostrar cuál fue su elección.
- Selección de una interface apropiada, con un fuerte análisis de alternativas y una fundamentación sobre la elección. Esto supone un desafío relacionado con características tales como la usabilidad y accesibilidad, pero sobre todo debe tener en cuenta que del diseño dependen determinados comportamientos electorales. En efecto, el formato final de la interfaz no es trivial. Según [10], "Es lógico esperar que la tecnología que se utiliza y las características específicas de la misma tengan un efecto potencial sobre el comportamiento de los actores que interactúan con ella".

b. Modelo basado en One Time Pad (OTP-Vote)

El modelo OTP- Vote se describe en [11] y focaliza especialmente en la confidencialidad e integridad de los datos de un sistema de voto electrónico. Se basa en la siguiente premisa fundamental: en los sistemas de voto electrónico es necesario proteger:

- Indefinidamente, la privacidad del votante, aún después de finalizada la elección.
- Mientras dure el proceso electoral, la seguridad de los datos de los votos, luego la información se hace pública.

El modelo hace uso de:

Claves One Time Pad, que cumplen con las hipótesis y condiciones del "Secreto Perfecto" de Shannon [12]: son aleatorias y tan largas como el mensaje.

Archivos de Datos que Almacenan Bits, que son elementos básicos en el modelo propuesto y se modifican en el transcurso del proceso, ellos son:

• Archivo Binario de Votos (ABV) cuya generación está basada en el modelo de almacenamiento Múltiples Canales Dato Único (MCDU) propuesto por García en [13], que se analiza en [14] y [15] y surge como una propuesta de resolución a las limitaciones de Birthday Paradox [16].

• Clave de Descifrado (CD): surge a partir de operaciones XOR (⊕) [17] de claves OTP.

Tablas Relacionales: que almacenan los datos de la configuración de la elección, cargos, candidatos e identificadores de votos y de los votos planos resultantes del proceso eleccionario.

El modelo propone:

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

El proceso incluye las etapas de:

- Configuración de la elección.
- Desarrollo de la elección.
- Cierre de la elección y recuento de votos.

El modelo teórico presentado supone, para cada una de las etapas mencionadas, el cumplimiento de algunas condiciones que resultan imprescindibles para alcanzar el normal funcionamiento del sistema. Estas condiciones se relacionan con aspectos tales como:

- La inalterabilidad de algunos elementos de datos durante el desarrollo del proceso electoral.
- El control de modificación de algunos elementos por determinados procesos.
- El desarrollo del proceso de auditoría en las diferentes etapas.
- El aseguramiento de la comunicación entre usuario y sistema en los momentos en que la misma se produce.
- El aseguramiento de la comunicación que realiza la transmisión de datos entre estaciones y servidor.

El modelo requiere entonces de la especificación de los puntos mencionados, para demostrar que el sistema resultante de la investigación es confiable y seguro.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

El grupo de trabajo investiga, básicamente sobre dos líneas paralelas para generar modelos que pudieran aplicarse a los sistemas de voto electrónico:

- Basados en criptografía homomórfica, que es la línea a cargo del Magíster Pablo Marcelo García.
- Basados en criptografía One Time Pad, que es la línea que lleva adelante la Magíster Silvia Gabriela Bast.

3. RESULTADOS Y OBJETIVOS

Los avances del grupo de trabajo que han surgido durante 2019 fueron:

a. En el ámbito de la criptografía homomórfica, este grupo de trabajo ha realizado las siguientes acciones:

   - Análisis de los resultados obtenidos en una encuesta online destinada a personas de todo nivel (desde expertos informáticos hasta votantes comunes) para obtener opiniones sobre la forma concreta que debería tener la interface de un sistema de voto electrónico.
   - Desarrollo de una serie de entrevistas a expertos informáticos para complementar los resultados obtenidos en la encuesta online. Esto se está realizando en la actualidad.
   - Incorporación al proyecto de dos especialistas específicos en comunicaciones de datos para proporcionar metodologías de transmisión de datos que garanticen los niveles de seguridad

exigibles. Los mismos se encuentran realizando el análisis de alternativas para implementar un esquema de basado en Virtual Nets. El objetivo será proporcionar un modelo de comunicación que cumpla con los requisitos.
- Se continuó trabajando en el análisis de métodos homomórficos existentes, avanzando en la selección final del esquema definitivo.

A futuro, se pretende llevar a cabo las siguientes acciones:

- Elegir la interface exacta del modelo en base a los datos obtenidos en encuestas y entrevistas.
- Aplicar la interface seleccionada y publicar los fundamentos de la selección.
- Definir un modelo de transmisión de datos e implementarlo.
- Realizar un relevamiento de aplicaciones orientadas al voto electrónico, que permita detectar falencias y proponer mejoras en el nuevo modelo.
- Selección de un método basado en criptografía homomórfica para aplicar en una futura implementación.

b. En cuanto a la línea de OTP Vote se ha avanzado sobre:
   - Aspectos de auditoría del modelo en cada una de las etapas del proceso.
   - Propuesta de Verificabilidad End to End.
   - Mejoras de la integridad de datos en el modelo, mediante la inclusión de bits de control que permiten verificar la integridad de los datos y detectar posibles intentos de intrusión. Modelo OTP-Vote
   - Se profundizó el trabajo sobre el refinamiento de los procesos de recuperación y generación de votos planos.

Se continuará avanzando en esta línea de investigación en aspectos tales como:

- Aseguramiento de la comunicación entre usuario-sistema y sistema-servidor de datos
- Refinamiento de la propuesta de modelo de auditoría de terceros.
- Automatización del proceso de generación de las tablas relacionales.
- Refinamiento de la propuesta de Verificabilidad End to End.

4. FORMACIÓN DE RECURSOS HUMANOS

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

- Pablo García y Silvia Bast completaron el cursado de la totalidad de los créditos exigidos en el Doctorado en Ingeniería Informática en la Facultad de Ciencias Físico Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL).
- Pablo García y Silvia Bast presentaron las modificaciones oportunamente exigidas a su Plan de Tesis Doctoral, en el marco del Doctorado en Ingeniería Informática en la Facultad de Ciencias Físico Matemáticas y Naturales de la Universidad Nacional de San Luis (UNSL). Las mismas se encuentran en proceso de evaluación.

5. BIBLIOGRAFÍA

[1] **McGaley M., Gibson J.:** "A critical analysis of the council of Europe recommendations on e-voting". EVT'06: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop

2006 on Electronic Voting Technology Workshop. 2006.
[2] 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. 2013.http://sedici.unlp.edu.ar/handle/10915/27537.
[3] **El Gamal T**. "A public key cryptosystem and a signature scheme based on discrete logarithms". In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10–18. Springer-Verlag New York, Inc. 1985.
[4] **Benaloh, J.:** "Dense Probabilistic Encryption". Workshop on Selected Areas of Cryptography. pp. 120–128. 1994.
[5] **O'Keeffe M.**: "The Paillier Cryptosystem: A Look Into The Cryptosystem And Its Potential Application". The College of New Jersey Mathematics Department. 2008.
[6] **Gentry G.:** "Fully Homomorphic Encryption Using Ideal Lattices". In the 41st ACM Symposium on Theory of Computing (STOC), 2009.
[7] **Hao, F, Ryan P.:** "Real -World Electronic Voting. Design, Analysis And Deployment". Cr Press. ISBN-13: 978- 1498714693. ISBN-10: 1498714692. 2017.
[8] **Rivest R**.: "On the notion of 'software independence' in voting systems". Philosophical Transactions of The Royal Society A, 366(1881):3759–3767. 2008.
[9] **Kelsey J., Regenscheid A., Moran T., Chaum D.**: "Attacking Paper-Based E2E Voting Systems". In: Chaum D. et al. (eds).
[10] **Ruiz Nicolini, J.:** "La(s) boleta(s) única(s)".https://www.elestadista.com.ar/?p=7104. 2015.
[11] **Bast S:**. "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. https://www.eae-publishing.com-ISBN 978-3-639-53793-2. 2017.
[12] **Shannon, C.:** "Communication Theory of Secrecy Systems" - Bell System Technical Journal - 1949.
[13] **García, P.**: "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] **van de Graaf J., Montejano G., García P.**: "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. Disponible en: http://42jaiio.sadio.org.ar/proceedings/simposios/Trabajos/WSegI/03.pdf. 2013.
[15] **García P., Montejano G., Bast S., Fritz E.:** "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.
[16] **García, P., van de Graaf J., Hevia A., Viola A.**: "Beating the Birthday Paradox in Dining Cryptographers Networks". En "Progress in Cryptology – Latincrypt 2014". Springer International Publishing. ISSN: 0302-9743. ISSN (electrónico): 1611-3349. ISBN: 978-3-319-16294-2. ISBN (eBook): 978-3-319-16295-9. Ps. 179 – 198. Octubre, 2014.
[17] **Murdocca M., Heuring V**. "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