Aspectos de Seguridad en Sistemas de Voto Electrónico

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

Las discusiones acerca de la aplicación del Voto Electrónico en Argentina se han profundizado en los últimos tiempos. Si bien existen grandes cuestionamientos sobre el uso de la tecnología en los procesos electorales, la idea de desarrollar un sistema de voto electrónico que cumpla con las características de anonimato y transparencia, no parece inviable si se aplican las condiciones de seguridad apropiadas. Es imprescindible que todos los ciudadanos perciban de manera incontrastable la transparencia del proceso; eso implica que cada votante pueda verificar los resultados y a la vez, alcanzar un convencimiento total de que el proceso se llevó a cabo de manera totalmente confiable.

Los investigadores del proyecto "Aspectos de en Seguridad en Proyectos de Software" desarrollan en paralelo dos modelos 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 uno de los modelos.

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

CONTEXTO

Este trabajo se enmarca en el Proyecto de Investigación: "Aspectos de Seguridad en Proyectos de Software", que se desarrolla en el ámbito de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa (UNLPam) Resolución N° 488/14 del Consejo Directivo de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa (FCEyN - UNLPam) 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 Licenciado Adrián García y al Programador Superior Claudio Ponzio como investigadores.

Surge desde la línea de Investigación "Ingeniería de Software y Defensa Cibernética", presentada en [1], 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

El modelo deberá cumplir con una serie de requisitos [2] que se exigen actualmente a los sistemas de votación electrónica:

- Evidencia física que garantice la transparencia del proceso [3]. En la mayoría de los casos, los nuevos sistemas son híbridos, es decir que producen un voto impreso que se utiliza como garantía de seguridad.
- 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. En este modelo se analizan alternativas basadas en esquemas homomórficos como Paillier [4], [5] o ElGamal exponencial [6], [7].
- Aplicación del concepto de independencia del software [8].
- Definir un modelo concreto para la aplicación de verificabilidad "End to End" (E2E) [9], [10].
- Aplicación de técnicas que eviten que un votante pueda demostrar por quién votó.

Los avances realizados en el proyecto durante 2018 se relacionan con tres aspectos:

- Análisis de la criptografía concreta que se va a aplicar en el modelo.
- Estudio de la forma exacta en que deben realizarse las comunicaciones de datos en el modelo de voto electrónico propuesto.
- Definición de una interface apropiada.

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

Este modelo teórico se concentra en los aspectos de confidencialidad e integridad de los datos de un sistema de voto electrónico [11] y se basa en la siguiente premisa fundamental: En los sistemas de voto electrónico es necesario proteger:

- De manera indefinida la privacidad del votante, aún después de finalizada la elección, dado que en caso de que algún intruso obtenga una copia digital de registros que permitan relacionar al votante con su voto contará con todo el tiempo para intentar descifrarlo.
- La seguridad de los datos de los votos mientras dure el proceso electoral, dado que luego la información se hace pública.

El modelo propuesto hace uso de:

- **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).
- **El esquema de almacenamiento denominado Múltiples Canales Datos único (MCDU)** y sus fórmulas propuestas para alcanzar dimensiones con comportamiento óptimo [13] y [14], aplicando operación XOR con la redundancia apropiada [15] para el almacenamiento de los datos.

El modelo asegura:

- Anonimato incondicional.

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

El proceso eleccionario se lleva a cabo en tres grandes etapas:

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

Los datos que están incluidos en los procesos son:

- Claves: Claves de las Autoridades (*CA*), Clave del Voto (*CV*) y Clave de Descifrado (*CD*).
- Archivos binarios de datos: Archivo Binario de Votos (*ABV*) y Archivo Binario de Votos Descifrado (*ABVD*)
- Tablas relacionales: IdVotos, Candidatos, Cargos, Atributos, Ubicaciones, Votos Planos

Para que el modelo teórico pueda ser efectivamente implementado, deben resolverse aspectos tales como:

- La seguridad de las *CA* que intervienen en el proceso.
- La inalterabilidad del *CV* que se genera como parte del proceso de desarrollo de la elección, en dos aspectos:
    - su almacenamiento mediante XOR en la *CD*.
    - como aporte a la Contribución Final del Voto que modificará finalmente el *ABV*.
- La confidencialidad e integridad en las tablas relacionales involucradas.
- *ABV* y *CD* deben ser accedidos y modificados sólo por el sistema de la forma propuesta por el Modelo.
- Propuesta del proceso de auditoría.
- Análisis de la semántica de los datos del voto, para incorporar atributos de control y de encriptación, variaciones en los datos almacenados de los votos y profundización de las posibilidades de recuperación semántica de los bits en las tuplas.
- Generación de un mecanismo que, teniendo en cuenta la semántica de los datos de voto (que es configurable y puede variar entre elecciones) facilite la generación de las tablas relacionales resultantes.
- Asegurar la comunicación entre el usuario y el sistema en los momentos en que la misma se produce y la transmisión de datos entre estaciones y servidor.

Una vez que los puntos mencionados estén resueltos, será posible 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 Magister Pablo Marcelo García.
- Basados en criptografía One Time Pad, que es la línea que lleva adelante la Magister Silvia Gabriela Bast.

3. RESULTADOS Y OBJETIVOS

Los avances del grupo de trabajo que han surgido durante 2018 son:

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

    - Una encuesta online para obtener respuestas de personas de todo nivel (desde expertos informáticos hasta votantes comunes) para recabar opiniones sobre la forma exacta que debería tener la

interface de un sistema de voto electrónico.
- Se incorporan al proyecto 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 en proceso de investigación para proporcionar un modelo de comunicación que cumpla con los requisitos.

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

- Aplicar la interface seleccionada al modelo a implementar.
- Desarrollar el modelo de transmisión de datos e implementarlo en la aplicación final.
- Realizar un permanente relevamiento de aplicaciones orientadas al voto electrónico, que permita detectar falencias y proponer mejoras en el nuevo modelo.

b. Con respecto a la línea de OTP Vote se ha avanzado sobre:

- El estudio de la semántica de los datos del voto, generando una propuesta de almacenamiento de los datos, que incluye atributos de control y de encriptación, variaciones en los datos almacenados de los votos, que apunta a oscurecer el contenido de los mismos para otorgar así, mayor seguridad al proceso eleccionario.
- El refinamiento de los procesos de recuperación y generación de votos planos [16]. Éste último mismo incluye un parser que, dada la configuración de los datos de la elección, que se establecen en la etapa inicial del proceso, genera la tabla de Votos Planos a medida que va realizando la recuperación de los sufragios emitidos por los electores.

Se continuará trabajando dentro de esta línea de investigación con aspectos tales como:

- Aseguramiento de la comunicación entre usuario-sistema y sistema-servidor de datos
- Propuesta de modelo de auditoría de terceros.
- Automatización del proceso de generación de las tablas relacionales.
- 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 asistió a un encuentro de tutoría con sus directores de Tesis Doctoral el Dr. Germán Montejano (UNSL) y Jeroen van de Graaf, PhD. (UFMG), en el ámbito de la FCFMyN (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] **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

[2] **Hao, F, Ryan P.:** "Real -World Electronic Voting. Design, Analysis And Deployment". Cr Press. ISBN-13: 978- 1498714693. ISBN-10: 1498714692. 2017.

[3] **Prince, A.:** "Consideraciones, Aportes y Experiencias para el Voto Electrónico en Argentina". Editorial Dunken. ISBN: 978-987-02-1732-9. 2006.

[4] **Volkhausen T.**: "Paillier Cryptosystem: A Mathematical Introduction". 2006.

[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] **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.

[7] **Koscielny C.**: "A New Approach to the Elgamal Encryption Scheme". Academy of Management of Legnica, Faculty of Computer Science. 2004.

[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] **Benaloh J. Bernhard M. Halderman J. Rivest R Ryan P. Stark P. Vora P. Teague V. Wallach D**.:"Public Evidence from Secret Ballots". Documento presentado en EVote-ID 2017.

[10] **Kelsey J., Regenscheid A., Moran T., Chaum D.**: "Attacking Paper-Based E2E Voting Systems". In: Chaum D. et al. (eds).

[11] **Bast S.:** "Optimización de la Integridad de Datos en Sistemas de E-Voting". Tesis de Maestría defendida en la Universidad Nacional de San Luis. 14 de diciembre de 2016. San Luis, Argentina.

[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] **Bast S., García P., Montejano G.:** "Refinamiento de los Procesos de Recuperación de Sufragios y Generación de Votos Planos en OTP-Vote" Congreso Nacional de Ingeniería en Informática / Sistemas de Información. CoNaIISI 2018.Universidad CAECE – Mar del Plata, Buenos Aires, Argentina. Publicación on line - ISSN 2347-0372