Anonimato en Sistemas de e-Voting: Últimos Avances

Pablo García[1,] Germán Montejano [1 2]; Silvia Bast[1]; Estela Fritz[1]

[1] Departamento de Matemática
Universidad Nacional de La Pampa
Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina
Tel.: +54-2954-245220– Int. 7125
[pablogarcia, silviabast, fritzem]@exactas.unlpam.edu.ar

[2] Departamento de Informática
Universidad Nacional de San Luis
Ejército de los Andes 950 – (5700) San Luis – San Luis – Argentina
Tel.: +54-266-4520300– Int. 2128
gmonte@unsl.edu.ar – web: http://www.unsl.edu.ar

Resumen

Desde el año 2012 se trabaja en la investigación relacionada con la protección de la privacidad de los votantes en un sistema de e-Voting. En ese sentido, se plantea que debe ser de mayor nivel la protección del anonimato que la que se le otorgue al proceso electoral, dado que este último debe ser protegido por un período finito de tiempo, mientras que el anonimato debe asegurarse indefinidamente.

En consecuencia, se considera probado que el nivel de seguridad para el anonimato debe ser incondicional, es decir que será seguro aún cuando un criptoanalista cuente con tiempo y recursos ilimitados. En cambio, puede aceptarse que al proceso de elección se le otorgue un nivel de seguridad computacional de razonable magnitud, teniendo en cuenta que luego de unas pocas horas, los resultados serán conocidos públicamente.

Fundamentalmente, los avances se relacionan con optimizaciones obtenidas sobre el protocolo Non-Interactive Dining Cryptographers (NIDC, [1]) el cuál es un derivado de [2], que incorpora características asíncronas.

En el presente documento se exponen los avances realizados en los últimos doce meses en el ámbito de la protección del anonimato y se enuncian las acciones futuras a desarrollar.

Palabras clave: ***Anonimato,*** **e-Voting,** ***Non–Interactive Dining Cryptographers, Seguridad Incondicional.***

Contexto

Por Resolución N° 488/14 del Consejo Directivo de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa se acredita el Proyecto de Investigación: "Aspectos de Seguridad en Proyectos de Software", que se desarrolla en el ámbito de la FCEyN de la UNLPam. El mismo es dirigido por el Doctor Germán Antonio Montejano y codirigido por el Magister Pablo Marcelo García e incluye a la Licenciada Silvia Gabriela Bast y la Profesora Estela Marisa Fritz como investigadoras.

El Proyecto surge desde la línea de Investigación "Ingeniería de Software y Defensa Cibernética", presentada en [3], y 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 Fisíco - Matemáicas 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).
Entre tales acciones debe mencionarse que Jeroen van de Graaf, PhD., Docente de UFMG, y el Dr. Germán Montejano (UNSL) fueron orientadores del Mg. Pablo García en el desarrollo de su tesis de maestría titulada "Optimización de un Protocolo Dining Cryptographers Asíncrono", defendida en 2013. Durante el desarrollo de la misma se generaron una serie de publicaciones de avances parciales, como por ejemplo [4], [5], [6], [7] y [8].

Introducción

El voto electrónico como alternativa al método manual tradicional presenta partidarios y detractores, en proporciones similares. Ambas posturas proponen argumentos razonables.

En consecuencia, la implementación de sistemas de voto electrónico exige que el escrutinio asociado refleje de manera indiscutible la voluntad de los ciudadanos y que, simultáneamente, los electores vean garantizada su privacidad de manera indefinida.

En particular, desde este proyecto se presta máxima atención a las consecuencias que puede acarrear, para cualquier votante, el hecho de que su voto se conozca. Fundamentalmente, a las prácticas deshonestas que se derivan de conocimiento de esa información. Tales prácticas pueden producirse con o sin el aval del elector. Por ejemplo, si un ciudadano pudiera probar que votó a un determinado partido político, podría obtener una contraprestación. Del mismo modo, si un sector detecta que un votante votó a otra opción, podría llevar a cabo acciones que perjudiquen al mismo.

Como consecuencia de lo anterior, la investigación otorga máximo interés a los protocolos que garanticen el anonimato incondicional y no exijan la concurrencia online de la totalidad de los participantes. NIDC cumple con ambos requisitos; es por este motivo que se trabajó en la optimización de algunos aspectos de la propuesta original:

- Nuevo protocolo antifraudes, basado en logaritmos discretos y commitments de Pedersen, que se presenta en [4] y que mantiene el nivel de seguridad original, (basado en BCX), con una mayor eficiencia en el uso de los recursos
- Esquema alternativo de almacenamiento de sufragios basado en canales paralelos de slots, que exige menor cantidad de almacenamiento ofreciendo para otorgar un nivel de seguridad determinado. Este esquema se presenta originalmente en [7].
- Implementación de múltiples redes NIDC en serie o paralelo con fines similares al párrafo anterior ([8]).

Líneas de Investigación, Desarrollo e Innovación

El grupo de trabajo investiga, básicamente sobre tres campos relacionados:

- Protección del anonimato de los votantes en sistemas de voto electrónico ([9]).
- Integridad de los datos de un sistema de e-Voting ([10]).
- Integridad de las bases de datos pertenecientes a un sistema de gestión de aprendizaje ([11]).

Resultados y Objetivos

En el ámbito de la protección de la privacidad, este grupo de trabajo ha realizado las siguientes publicaciones:

- [12]: Presenta una técnica basada en almacenamiento de sufragios basada en canales paralelos de slots, exponiendo una serie de fórmulas matemáticas que describen el comportamiento del mismo.
- [13]: Este documento expone un método sistemático de elección de los parámetros óptimos para la implementación de un esquema del tipo descripto en el párrafo anterior.
- [14]: Muestra una generalización del enfoque basado en canales paralelos y muestra los resultados obtenidos con la implementación de un simulador de actos eleccionarios.

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

- Implementación de una aplicación experimental que permita observar el comportamiento de los modelos propuestos en las publicaciones producidas, tanto en lo referido a la protección de la privacidad como a la seguridad de las bases de datos relacionadas con un sistema de voto electrónico.
- Continuar con el relevamiento de aplicaciones orientadas al voto electrónico, con el fin de detectar falencias y proponer mejoras.
- Ampliar el simulador de actos eleccionarios para su generalización y publicación online.

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 Universidade 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 mayo de 2016. 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 septiembre de 2015. 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).

- Silvia Bast y Pablo García 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).
- Estela Fritz está desarrollando su tesis para obtener el grado de “Especialista en Tecnologías Informáticas aplicadas en Educación”. Su plan de trabajo fue aprobado y se planea su defensa para octubre de 2016. La tesis se titula “Propuesta de clasificación de software libre utilizado en la enseñanza de la programación” y es dirigida por Mg. Alejandra Zangara (UNLP).

Referencias

[1] van de Graaf J.: ”Anonymous One Time Broadcast Using Non Interactive Dining cryptographer Nets with Applications to Voting”’. Publicado en: ”Towards rustworthy Elections”. Ps 231-241. Springer-Verlag Berlin, Heidelberg. ISBN:978-3-642-12979-7. 2010.

[2] Chaum D.:”The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability”. Journal ofCryptology. 1988.

[3] 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 Workshop de Investigadores en Ciencias de la Computación 2013 (WICC 2013). Ps.769 - 773. ISBN: 9789872817961. 2013.

[4] 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 y 22 de noviembre de 2013. Córdoba, Argentina. NACIONAL.

[5] van de Graaf J., Montejano G., García P., Bast S.: “Anonimato en Sistemas de Voto Electrónico”. Memorias del XVI Workshop de Investigadores en Ciencias de la Computación 2014 (WICC 2014). Ps. 822 – 826. ISBN: 9789503410844 . 8 y 9 de mayo de 2014. NACIONAL.

[6]. 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). Ps. 29 a 43. Septiembre 2013. NACIONAL.

[7] 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). Trabajo en aceptado para su presentación. NACIONAL.

[8] García P., van de Graaf J., Hevia A., Viola A.: “Beating the Birthday Paradox in Dining Cryptographer Networks”. The third International Conference on Cryptology and Information Security in Latin America, Latincrypt 2014. September 17-19, 2014. Florianopolis, Brasil. Lecture Notes in Computer Science, Springer (2014). INTERNACIONAL.

[9] García P., Montejano G., Bast S., Fritz E.: “Seguridad Incondicional para el Anonimato en Sistemas de e-Voting”. XVII Workshop de Investigadores en Ciencias de la Computación (WICC 2015). 16 y 17 de abril de 2015. Facultad de Ciencias Exactas. Universidad Nacional de Salta. ISBN: 978-987-633-134-0. NACIONAL.

[10]. Bast S., Montejano G., García P., Fritz E.: “Evaluación de la integridad de datos en Sistemas de e-Voting”. XVII Workshop de Investigadores en Ciencias de la Computación (WICC 2015). 16 y 17 de abril de 2015. Facultad de Ciencias Exactas. Universidad Nacional de Salta.ISBN: 978-987-633-134-0. NACIONAL.

[11] Fritz E., Montejano G., García P., Bast S.,: ”Integridad de Datos en Sistemas de Gestión de Aprendizaje”. XVII Workshop de Investigadores en Ciencias de la Computación (WICC 2015). 16 y 17 de abril de 2015. Facultad de Ciencias Exactas. Universidad Nacional de Salta. ISBN: 978-987-633-134-0. NACIONAL.

[12] García P., van de Graaf J., Montejano G., Riesco d, Debnath N., Bast S.: ”Storage Optimization for Non Interactive Dining Cryptographers (NIDC)”. 12th International Conference onInformation Technology : New Generations (ITNG 2015). April 13-15, 2015, Las Vegas, Nevada, USA.

[13] García P., van de Graaf J., Montejano G., Riesco D., Debnath N., Bast S.:“A Systematic Method for Choosing Optimal Parameters for Storage in Parallel Channels of Slots”. 2016 IEEE International Conference on Industrial Technology (ICIT2016). 14-17 de marzo de 2016. Taipei, Taiwan. Trabajo aceptado para su publicación. Previamente el trabajo fue aceptado en NICS 2015, AICCSA 2015 y 12th ACS/IEEE International Conference on Computer Systems and Applications, pero no fue publicado por falta de financiación.

[14] García P., Montejano G. Bast S., Fritz E., Riesco D., Debnath N.,: ”A Proposal for Anonymous Data Storage”. IEEE International Conference on Industrial Informatics. INDIN 2016. 18 al 21 Julio de 2016, Futuroscope-Poitiers, Francia. Trabajo enviado para su evaluación.