Seguridad Incondicional para el Anonimato en Sistemas de e-Voting

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.: +54-2652-424027 – Int. 251
gmonte@unsl.edu.ar – web: http://www.unsl.edu.ar

Resumen

En el ámbito de los esquemas de voto electrónico, el nivel de seguridad que se otorga al anonimato del elector se encuentra, en muchas ocasiones en un nivel inferior con respecto a la que se brinda al proceso eleccionario en sí. Por ejemplo, todos los esquemas basados en Mix - Net proporcionan seguridad computacional para el anonimato e incondicional para el proceso electoral.

Sin embargo, es ilógico proteger de manera incondicional un proceso que dura un tiempo limitado y otorgar, simultáneamente, seguridad computacional a información que debería ser mantenida en secreto indefinidamente. Como consecuencia de tal observación es que surge en 2012 una línea de investigación para trabajar sobre este tópico, teniendo como objetivo central definir de manera precisa cuál es el nivel de seguridad que debe otorgarse al anonimato de un elector.

A esta altura se considera probado que es necesario proveer de seguridad incondicional a la privacidad de los electores.

Este documento expone los avances realizados hasta el momento y presenta las futuras acciones a desarrollar.

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

Contexto

El presente 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 y en el Proyecto de Investigación "Ingeniería de Software, Conceptos, Métodos y Herramientas en un Contexto de Ingeniería de Software en Evolución" de la Universidad Nacional de San Luis.

Introducción

Una característica muy marcada de estos tiempos es la velocidad con que las innovaciones tecnológicas se produ-

cen. Resulta muy difícil seguir el ritmo de las novedades, sobre todo en lo referido a la aparición de nuevos dispositivos, conceptos, y siglas, que nacen como consecuencia del proceso de innovación permanente.

Entre miles de ejemplos, podemos mencionar: el geométrico avance en la capacidad de los procesadores (fundamentalmente por la implementación de núcleos y el multiprocesamiento resultante), la permanente aparición de nuevos dispositivos, el aumento en la cantidad de memoria provista con los equipos o la diversificación de los elementos de entrada / salida, aspecto que no parece tener límites y que promete alcanzar niveles que poco tiempo atrás hubiesen resultado impensados.

Lo mismo ocurre en el ámbito de la seguridad informática en general y en la criptografía en particular. Una de las razones de este fenómeno pasa por el gran aumento del volumen de información disponible. Cualquier nuevo método que aparece es rápidamente puesto a disposición de una enorme masa crítica que evalúa y genera los cambios que considera necesarios. Simultáneamente, el crecimiento geométrico de la capacidad de ataque de un criptoanalista exige que un sistema criptográfico demuestre su seguridad de manera indiscutible, debiendo aplicarse rigurosas técnicas matemáticas formales.

Una de las aplicaciones con mayores exigencias en ese sentido es el Voto Electrónico. Los resultados de una votación definen importantes relaciones de poder y el manejo de importantes recursos económicos. En consecuencia, es imprescindible asegurar dos puntos fundamentales:

- El escrutinio debe reflejar de manera transparente la voluntad de los ciudadanos.
- Un votante debe contar con la garantía de que su voto se mantendrá anónimo indefinidamente.

Es obvio que lo que se pone en juego en un acto eleccionario presenta la suficiente importancia como para que aparezcan todo tipo de conductas deshonestas. Algunas de ellas apuntan a alterar el resultado del escrutinio. Sin embargo, a los efectos de esta investigación, resultan de interés aquellas que se relacionan con la vulnerabilidad del anonimato de un elector. Por ejemplo, las derivadas de lo que se conoce como *clientelismo político*, es decir aquellas acciones que los partidos políticos puedan ejercer en busca de obtener un voto a cambio de algún tipo de contraprestación.

Es fundamental que el anonimato de un votante se mantenga eternamente. Es fácil imaginar las consecuencias que podría generar en cualquier ciudadano el hecho de que el vencedor de la elección sepa que un elector votó a la oposición.

Tradicionalmente, se ha considerado a la privacidad como un valor mucho menos importante que la legitimidad de los resultados. Si bien es evidente la enorme relevancia que implica asegurar un recuento correcto, queda claro que el nivel de importancia que debe darse a la privacidad es similar. En la presente investigación se busca definir la manera exacta en que el anonimato debe ser administrado.

Si se desea generalizar la utilización del voto electrónico, debe demostrarse que las prestaciones que provee son superiores a las que se puedan obtener en un sistema manual. En ese sentido, es claro que no existe acuerdo en la comunidad académica sobre la conveniencia del E-Voting. Por ejemplo: [1] presenta fuertes críticas a la implementación del voto electrónico y se puede obtener un panorama completo de potenciales problemas y sus soluciones aplicables en [2].

Para este documento en particular, se analizan exclusivamente los aspectos relacionados con el aseguramiento de la privacidad de un elector. Debe observarse, además, que existen una serie de cuestiones adicionales que deben tenerse en cuenta. Por ejemplo, un esquema totalmente online no puede garantizar que el votante se encuentra solo en el momento de votar, en consecuencia podría recibir presiones que deriven en una elección ajena a sus preferencias. Es el caso de Helios, Opa-Vote y otros productos que fueron evaluados como parte de esta investigación.

En un esquema presencial, una medida crucial para mantener el anonimato de un votante honesto consiste en la separación de los procesos de identificación del elector (que debe garantizar que se trata de un votante habilitado que no haya votado previamente) y el de votación específico (que debería realizarse en base a un código totalmente aleatorio, que sólo conocerá el votante y que no tendrá relación alguna con el documento de identidad).

Helios u Opa Vote, proponen un modelo totalmente remoto. En consecuencia, su esquema no resulta generalizable a grandes elecciones porque se hace imposible garantizar la ausencia de cohersión. Tal característica es simple de implementar en un esquema presencial: la soledad del votante al momento de sufragar otorga garantías razonables. Cabe mencionar que ambos productos advierten claramente al usuario al respecto.

Todos los modelos analizados parecen ofrecer condiciones seguras para un votante honesto. Si se proporciona un código de control con una posterior publicación on-line, el sistema resulta transparente.

Sin embargo, el mayor inconveniente radica en evitar que un voto resulte marcado. El votante podría indicar su código a un partido político para reclamar alguna contraprestación. En cualquier caso, todos los modelos electrónicos analizados dificultan tal maniobra. En efecto, marcar un voto en el esquema manual es muy simple, escribiendo algo que fue pactado de antemano. Realizar una maniobra de ese estilo en los esquemas electrónicos observsdos resulta más dificultoso.

Además del análisis de productos, la investigación ha hecho aportes sobre modelos teóricos existentes, punto que se detalla en la siguiente sección.

Líneas de Investigación, Desarrollo e Innovación

En desarrollos previos se ha trabajado en profundidad sobre Dining Cryptographers de Chaum (DC, [3]) y su variante asíncrona: Non Interactive Dining Cryptographers (NIDC, [4]), que agrega un esquema basado en rondas y la utilización de firmas ciegas ([5]). La característica más relevante del esquema DC y sus derivados pasa por garantizar el anonimato incondicional de los participantes, como parte del funcionamiento del algoritmo que implementa.

Resultados y Objetivos

En el ámbito de esta línea de investigación se realizaron las siguientes publicaciones durante los últimos 12 meses:

- En [6] se propone una técnica de almacenamiento de sufragios basada en canales paralelos de slots, inspirado en NIDC, pero de aplicación más general. Se enuncian, además fórmulas matemáticas que definen:
  - Valor esperado de la variable “Cantidad de Sufragios Perdidos”.
  - Valor óptimo del parámetro “Cantidad de Slots que debe tener cada canal”.

    - Valor óptimo de la magnitud "Cantidad de Canales Paralelos" que deben implementarse.
    - Cota superior para la probabilidad de no perder votos en un esquema NIDC con aplicación de vectores replicados.
- En [7] se comparan los resultados obtenidos aplicando repeticiones secuenciales y paralelas de redes basadas en Dining Cryptographers.
- En [8] se propone una variante al protocolo antifraudes original de NIDC que genera una significativa mejora en la eficiencia del esquema, por implementación de logaritmos discretos y Commitments de Pedersen.
- En [9] se exponen avances relacionados con la optimización del almacenamiento utilizado en un esquema NIDC.

A futuro, se pretende trabajar en dos sentidos complementarios:

- Profundizar la investigación para obtener nuevas conclusiones tendientes a lograr implementaciones efectivas de productos de software basados en protocolo DC y derivados.
- Continuar con el relevamiento de aplicaciones orientadas al voto electrónico, con el fin de detectar falencias y proponer mejoras.

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 junio de 2015. 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 se encuentran cursando 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 diciembre de 2015. 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] Bunge T., Dankert I, and Grosso E.: El voto electrónico, esnobismo de la era cibernética. En: http://www.cema.edu.ar.

[2] Amurao D.: Computerized voting: Problems and solutions. SIGCAS Comput. Soc., pages 44–56, 2006.

[3] Chaum D.: "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability". Journal of Cryptology. 1988.

[4] van de Graaf J.: "Anonymous One Time Broadcast Using Non Interactive Dining Cryptographer Nets with Applications to Voting". Publicado en: "Towards Trustworthy Elections". Pages 231 - 241. Springer - Verlag Berlin, Heidel-berg. ISBN:978-3-642-12979-7. 2010.

[4] Fujioka A., Okamoto T., Ohta K.: "A Practical Secret Voting Scheme for Large Scale Elections". AUSCRYPT 1992. LNCS, Vol. 718. Páginas 244 a 251. Springer Heidelberg. 1993.

[6] - 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). ISSN/ISBN: 2313-9102.

[7] - 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).

[8] - García P., Montejano G., Bast S.: "Aspectos optimizables en un Protocolo Non-Interactive Dining Cryptographers". Segundo Congreso Nacional de Ingeniería Informática / Sistemas de Información (CONAIISI 2014). ISSN/ISBN: 2346-9927 13 de noviembre de 2014. Universidad Nacional de San Luis. San Luis, Argentina.

[9] - García P., van de Graaf J., Montejan G., Riesco D., Debnath N., Bast S.: "Storage Optimization for Non Interactive Dining Cryptographers (NIDC)". 12th International Conference on Information Technology: New Generations (ITNG 2015). April 13-15, 2015, Las Vegas, Nevada, USA. Trabajo aceptado para su publicación.