Anonimato en Sistemas de Voto Electrónico

Jeroen van de Graaf [1]; Germán Montejano[2 3]; Pablo García[3]; Silvia Bast[3]

[1]Departamento de Ciência da Computação - Universidade Federal de Minas Gerais

Av. Antonio Carlos, 6627 – 31270-010 - Belo Horizonte – Minas Gerais - Brasil

Tel.:+55-3409-5836

jvdg@dcc.ufmg.br – web: http://www.dcc.ufmg.br/~jvdg

[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

[3]Departamento de Matemática - Universidad Nacional de La Pampa

Av. Uruguay 151 – (6300) Santa Rosa – La Pampa – Argentina

Tel.: +54-2954-425166– Int. 125

[pablogarcia,silviabast]@exactas.unlpam.edu.ar – web:http:/unlpam.edu.ar

Resumen

En muchos esquemas de voto electrónico muy difundidos, la seguridad otorgada con respecto a la privacidad del votante se encuentra en un escalón inferior con respecto a la que se brinda al proceso eleccionario en sí. Para respaldar tal afirmación puede mencionarse que todos los esquemas conocidos que emplean Mix-Net proporcionan seguridad computacional para el anonimato e incondicional para el proceso electoral.

Tal asignación, en lo que respecta a niveles de seguridad, resulta ilógica. No parece razonable proteger de manera incondicional un proceso que dura unas pocas horas y otorgar, simultáneamente, seguridad computacional a información que debería ser mantenida en secreto indefinidamente.

Planteos como el expuesto dan lugar a la presente investigación.

En primer lugar se propone analizar el comportamiento, en ese sentido, de algunos de los esquemas más conocidos de voto electrónico, tales como Wombat, Scantegrity, Vot.ar, y Helios.

Teniendo en cuenta lo expuesto en el párrafo anterior, se busca encontrar elementos que parmitan definir el nivel de seguridad exacto que debe otorgarse a la privacidad.

Palabras clave: ***Voto electrónico, anonimato, privacidad, Dining Cryptographers, seguridad incondicional.***

Contexto

El presente trabajo se enmarca en el Proyecto de Investigación: "Ingeniería de Software: Aspectos de Alta sensibilidad en el ejercicio de la Profesión del Ingeniero de Software", dentro de la línea de investigación denominada “Ingeniería de Software y Defensa Cibernética presentada en WICC 2013 [1], que se desarrolla en el ámbito de la Facultad de Ciencias Físico-Matemáticas y Naturales de la Universidad Nacional de San Luis.

Introducción

La evolución de la tecnología ha modificado sustancialmente muchas cosas en la sociedad. Resulta sorprendente analizar los cambios que se han producido en los últimos años. La actualidad muestra una increíble velocidad a la hora de generar cambios. Aún para los profesionales informáticos resulta difícil mantenerse al día en lo que respecta a la aparición de nuevos dispositivos, conceptos, y siglas, que nacen como consecuencia del proceso de innovación permanente.

La velocidad antes mencionada se verifica en todo lo relacionado con la tecnología. Entre miles de ejemplos, podemos mencionar: la capacidad de los procesadores (con la optimización significativa que provoca la implementación de núcleos y el paralelismo resultante), la contínua aparición de nuevos dispositivos, el aumento en la cantidad de memoria provista con los equipos (tanto primaria como secundaria), la diversificación de los elementos de entrada / salida, y muchos más.

En particular, resulta de gran interés la manera en que esa dinámica también aparece, nítida, en lo relacionado a la seguridad informática en general y a 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 fuerza los cambios que considera necesarios. Ya no es suficiente con proclamar una supuesta seguridad: es necesario demostrar el nivel de la misma de manera matemática y formal.

En ese entorno se plantea la alternativa del voto electrónico, que se relaciona con un elemento fundamental: los procesos eleccionarios representan un elemento central en los países democráticos. Los resultados de una votación pueden definir, entre otras cosas, importantes relaciones de poder y manejo de significativos recursos económicos. En consecuencia, el escrutinio asociado debe reflejar de manera transparente la voluntad de los ciudadanos.

Sin embargo, el alto valor de los elementos en disputa, propicia la existencia de conductas deshonestas, entre las cuales se puede detectar algunas directamente relacionadas con el anonimato de los votantes:

- **Clientelismo político:** Existen prácticas relacionadas con la obtención de un voto a través de la entrega de algún tipo de contraprestación. Los partidos políticos, en ocasiones, realizan este tipo de maniobras. Si un votante pudiera demostrar de manera fehaciente cuál fue su elección, se vería favorecida la aplicación de estas maniobras.
- **Trayectoria del votante:** Ningún ciudadano honesto desea que se conozcan públicamente las opciones que seleccionó en procesos eleccionarios previos. En particular, un político podría

verse expuesto si se conociera su conducta en votaciones previas.

En definitiva, la privacidad del votante no es un elemento que pueda descuidarse. Por lo tanto, se intenta determinar el nivel exacto de seguridad que debe proveerse al anonimato.

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, no queda claro el nivel de importancia que debe darse a la privacidad. 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. No existe acuerdo en la comunidad académica sobre la conveniencia del E-Voting. Por ejemplo, [2] y [3], entre otros, son muy críticos con la implementación del voto electrónico. Un buen análisis de los reales alcances del E-Voting se presenta en [4], un estudio de las limitaciones en el caso de esquemas basados en Mix -Net se describe en [5] y un listado de potenciales problemas y sus soluciones se desarrolla en [6].

La comparación debe realizarse en todos los aspectos involucrados. Sin embargo, en esta linea en particular, se desea analizar exclusivamente el aspecto relacionado con el anonimato.

Es evidente que el nivel de seguridad que cada esquema proporciona es dependiente de la naturaleza del modelo. Por ejemplo, un esquema totalmente online no puede garantizar que el votante se encuentra solo en el momento de votar. En consecuencia, su voto podría no ser absolutamente privado, además de que podría existir cohersión.

Dentro de los modelos seleccionados para el análisis, sólo Helios es totalmente online. 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, en cambio, propone un modelo totalmente remoto. En consecuencia, el 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.

Todos los modelos presentados parecen ofrecer condicones 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 analizados resulta más dificcultoso.

Líneas de Investigación, Desarrollo e Innovación

En desarrollos previos se ha trabajado en profundidad sobre Dining Cryptographers de Chaum [7] y su variante asíncrona: Non Interactive Dining Cryptographers [8], que agrega un esquema basado en rondas y la utilización de firmas ciegas [9]. La principal característica de esos esquemas pasa por otorgar seguridad incondicional al anonimato.

Como consecuencia de lo anterior, surge naturalmente la idea de trabajar exclusivamente sobre el tema de la privacidad, analizando el estado del arte para, posteriormente, proponer nuevas metodologías.

Resultados y Objetivos

En el ámbito de esta línea de investigación se pueden mencionar los siguientes resultados:

- Fórmula para definir la cantidad óptima de canales paralelos con réplica en un esquema "Occuppancy Problem".
- Cota superior para la probabilidad de no perder votos en un esquema Dining Cryptographers asíncrono con aplicación de vectores replicados.
- Fórmula que define el valor esperado para el porcentaje de votos perdidos en una elección realizada con un esquema NIDC con canales paralelos
- Protocolo que optimiza el esquema Non – Interactive Dining Cryptographers, manteniendo seguridad incondicional.

Las cuatro referencias mencionadas se encuentran plasmadas en la tesis de maestría de Pablo García, con desarrollos parciales en [10], [11] y [12].

A futuro, se busca obtener nuevas conclusiones relacionadas específicamente con el anonimato en sistemas de voto electrónico.

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 2014. La tesis se titula: "Sistemas de E-Voting: Integridad de Datos" y está dirigi-da 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 junio de 2014. 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).

Referencias

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

[2] Bunge T., Dankert I, and Grosso E.: El voto electrónico, esnobismo de la era cibernética. En: http://www.cema.edu.ar.

[3] Fernández E., La Red D., Peláez J.: ¿son seguras las elecciones que usan maquinas electrónicas y la internet?. Technology Journal LAC, 1:171 – 180, 2012.

[4] Alam K., Tamura S.: Electronic voting - scopes and limitations. International Conference In Informatics, Electronics Vision (ICIEV), pages 525–529, 2012.

[5] Jakobsson M., Juels A, Rivest R.: Making mix nets robust for electronic voting by randomized partial checking. AUSENIX Security 02, 7:339–353, 2002.

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

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

[8] 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.

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

[10] van de Graaf J., Montejano G., García P.: "Optimización de un esquema Ocuppancy Problem orientado a E – Voting". Memorias del XV Workshop de Investigadores en Ciencias de la Computación 2013 (WICC 2013). Ps.749 - 753. ISBN: 9789872817961. 2013.

[11] van de Graaf J., Montejano G., García P.: "Manejo de Colisiones en un Protocolo Non Interactive Dining Cryptographers ". 42◦ Jornadas Argentina de Informática e Investigación Operativa (JAIIO, ISSN: 1850-2776). Workshop de Seguridad Informática (WSegI 2013, ISSN: 2313-9110). Ps.36 a 50. 2013.

[12] van de Graaf J., Montejano G., García P.: "Optimización de un Protocolo Non-Interactive Dining Cryptographers". 1er Congreso Nacional de Ingeniería Informática / Sistemas de Información. CoNaIISI 2013.