OTP-Vote: Avances en la Generación de un Modelo de Voto Electrónico

Silvia Bast[1]; Pablo García[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

En la actualidad, gran parte de las actividades humanas se ven mediadas por el uso de las plataformas tecnológicas. Resulta lógico pensar que con el transcurrir del tiempo, aún mayor cantidad de tareas irán migrando a su forma electrónica y permitirán que los usuarios las lleven a cabo de manera remota. Debido a los avances tecnológicos, al crecimiento poblacional y a las distancias geográficas, los sistemas de voto presentan un gran potencial para ser llevados a cabo parcial o totalmente de manera electrónica. Existen, sin embargo, cuestiones de confianza por parte de los ciudadanos en este tipo de sistemas, dado que contienen información sumamente sensible para el elector. La seguridad es entonces un aspecto central que debe reforzarse en tales sistemas. Básicamente debe ser posible mantener de forma anónima la información del voto de cada uno de los electores y debe resultar imposible modificar los votos ya emitidos.

Se plantean entonces problemas relacionados con la confidencialidad y la integridad de los datos

Se exponen en el presente documento los avances obtenidos en la investigación de un modelo que optimiza los aspectos de confidencialidad e integridad en Sistemas de Voto Electrónico.

El modelo propuesto se denomina: OTP-Vote.

Palabras clave: ***sistemas de voto electrónico, confidencialidad, integridad, seguridad.***

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 y es es dirigido por el Doctor Germán Antonio Montejano y codirigido por el Magister Pablo Marcelo García e incluye a la Mg. Silvia Gabriela Bast y la Profesora Estela Marisa Fritz como investigadoras.
Surge desde la línea de Investigación "Ingeniería de Software y Defensa Cibernética", presentada en [1], 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 Físico - 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. El Mg García ha realizado estadías de investigación en UFMG en 2013 mientras desarrollaba su tesis y en 2016 en el Laboratorio 4303 en el Departamento da Ciências da computação do Instituto de Ciências Exatas.

1. INTRODUCCIÓN

El voto electrónico puede definirse como *"una forma de votación basada en medios electrónicos que se diferencia del método tradicional por la utilización de tecnologías como hardware, software y procedimientos que permiten automatizar los procesos que comprenden unas elecciones"*[1]

En el ámbito del proyecto de investigación se propone una nueva metodología para aplicar a los sistemas de E-Voting, presentada en [2]. El desarrollo de la misma implicó llevar a cabo las siguientes actividades:

- Analizar las características y requerimientos de sistemas de Voto electrónico.
- Analizar las herramientas y modelos que focalizan en la seguridad de los datos.
- Proponer en base a los análisis realizados un modelo que optimice los aspectos de confidencialidad e integridad de los datos ofreciendo anonimato incondicional y seguridad computacional (que puede llevarse al nivel exigible) durante el proceso electoral.
- Aplicar el modelo a casos para validar su funcionamiento.

Los Requerimientos de los Sistemas de Voto Electrónico

Del análisis de las características de estos sistemas ([3], [4] y [5]), surge un grupo de requisitos que deben respetar los mencionados desarrollos. Los mismos pueden resumirse en: Anonimato, Autenticación del votante, Verificabilidad, Simplicidad, Costo, Auditabilidad, Inviolabilidad, Seguridad, No coerción, Robustez.
Entre los requerimientos mencionados, existen algunos que pueden satisfacerse de forma sencilla, pero otros presentan mayor nivel de dificultad. En los sistemas de Voto electrónico es necesario proteger:

- Indefinidamente la privacidad del votante: aún después de

[1] Sitio Observatorio del voto-E en América Latina disponible en http://www.voto-electronico.org/index.php/definicion/definicion-amplia

finalizada la elección, dado que en caso de que algún intruso obtenga una copia digital de registros que permitan relacionar el votante con su voto contaría con todo el tiempo para intentar descifrarlo. Las personas desean mantener su privacidad asegurada indefinidamente y existen casos en los que sería de suma gravedad que se conociera por quién votó alguna persona en particular. Por ejemplo, conocer la trayectoria como votante de un candidato actual podría influir en el electorado

- Mientras dure el proceso electoral, la seguridad de los datos: la protección de la información circulante sólo debe soportar el lapso de tiempo que corresponda al proceso de votación.

Aportes Teóricos para la Propuesta de un Modelo de Datos para Sistemas de Voto Electrónico.

El modelo propuesto se basa en:

1) El modelo de almacenamiento de Canales Paralelos – Múltiples Canales Dato Único (MCDU, [6], [7], [8], [9] y [10]), que ofrece :
- Anonimato Incondicional: a través de su característica de aleatoriedad.
- Uso eficiente del almacenamiento.
- Disminución de la probabilidad de colisiones, que puede llevarse a cualquier nivel exigible a través del uso de las fórmulas para la configuración de parámetros de la elección.

2) El uso de claves One Time Pad (OTP) [11]. OTP es un algoritmo criptográfico que puede crear un texto cifrado del que nadie puede obtener el texto plano y que no puede quebrarse aún con potencia de cálculo infinito e ilimitada cantidad de tiempo.

   Las claves OTP presentan las siguientes características:
- Son aleatorias.
- Son tan largas como el mensaje mismo.
- A partir del mismo texto cifrado, aplicando una clave diferente se produce un texto plano distinto.

3) El uso de la Redundancia Adecuada en la definición de las dimensiones de los atributos que formarán parte del Voto [12] con el objetivo de:
- Disminuir considerablemente la posibilidad de detectar cuáles son los valores válidos que se han usado.
- Disminuir también la probabilidad de que por el efecto de colisiones simples o múltiples, se produzca como resultado otro Identificador de voto válido.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Las líneas de investigación que se siguen son:

- Desarrollo de un modelo de datos que optimice las características de confidencialidad e integridad de los datos.
- Desarrollo de compromisos y protocolos que permitan asegurar que la información que es intercambiada se mantiene inalterable.
- Desarrollo de una técnica para verificabilidad E2E del modelo propuesto, basada en funciones de Hash.
- Implementación del sistema propuesto.

3. RESULTADOS Y OBJETIVOS

Se desarrolló un Modelo de Datos que ofrece:

- Anonimato Incondicional: aportado por: la aleatoriedad en el almacenamiento de datos del modelo subyacente, esto es, Canales Paralelos MCDU, las claves OTP que se usan para la encriptación y la separación total de los procesos de acreditación y emisión de voto.
- Seguridad Computacional que puede llevarse a cualquier nivel exigible a través de: la aleatoriedad en el almacenamiento de datos provista por el uso de Canales Paralelos MCDU, las claves OTP que se usan para la encriptación, el uso de la redundancia suficiente en los atributos de las tuplas y la configuración de los parámetros de la elección.

Se desarrollaron dos propuestas de recuperación de colisiones adicionales al modelo.

Se validó el modelo a través de su aplicación a diferentes casos generados por un simulador desarrollado ad-hoc.

Se espera avanzar en el refinamiento de protocolos antifraude [13] y en la implementación del modelo.

También se está trabajando para agregar a la propuesta, la característica 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 realizó una estadía de un año en la Universidad 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 defendió su tesis para obtener el grado de Magister en Ingeniería de Software de la Universidad Nacional de San Luis, bajo la dirección del Dr. Germán Montejano (UNSL) y del Mg Pablo García (UNLPam). La tesis se tituló: "Optimización de la integridad de datos en Sistemas de E-Voting" y recibió la calificación de Sobresaliente.
- 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 Agosto de 2017. 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 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 Agosto de 2017. La tesis se titula: Sistemas de E-Voting: Integridad de Datos" y es dirigida por el Dr. Germán Montejano (UNSL) y el Mg. Pablo García (UNLPam).
- Silvia Bast y Pablo García completaron el cursado del Doctorado en Ingeniería Informática en la Facultad de Ciencias Físico Matemáticas y Naturales de la

Universidad Nacional de San Luis (UNSL).

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] **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.

[3**] EPSTEIN J.:** "Electronic Voting", Cyber Defense Agency LLC.

[4**] KAZI M., ALAM R., TAMURA S.:** Electronic Voting - Scopes and Limitations IEEE/OSA/IAPR International Conference on Infonnatics, Electronics & Vision.

[5] **PRINCE A.:** Consideraciones, aportes y experiencias para el Voto electrónico en Argentina. 2005.

[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). Páginas 29 a 43. Septiembre 2013. Disponible en: http://42jaiio.sadio.org.ar/ proceedings/ Simposios/Trabajos/WSegI/ 03.pdf.

[7] **GARCÍA P., VAN DE GRAAF, MONTEJANO G., RIESCO D., DEBNATH N., BAST S.:** "Storage Optimization for Non-Interactive Dining Cryptographers (NIDC)". The International Conference on Information Technology: New Generations. 2015. Las Vegas, Nevada, USA. Disponible en: http://ieeexplore.ieee.org/document/711344 9/.

[8] **GARCÍA P., BAST S., FRITZ E., MONTEJANO G., RIESCO D., DEBNATH N.:** "A Systematic Method for Choosing Optimal Parameters for Storage Parallel Channels of Slots". IEEE International Conference on Industrial Technology (ICIT 2016). 14 - 17 March 2016 / Taiwan, Taipei. Disp. en: http://ieeexplore.ieee.org/document/747501 9/.

[9] **GARCÍA P., MONTEJANO G., BAST S., FRITZ, E.: "**Loss of Votes in NIDC Applying Storage in Parallel Channels". Congreso Argentino de Ciencias de la Computación, CACIC 2016. San Luis, 3 al 7 de octubre de 2016. Universidad Nacional de San Luis (UNSL). Se obtiene distinción como MEJOR EXPOSITOR del Workshop de Seguridad Informática. Seleccionado para ser publicado en el libro de los mejores artículos de CACIC 2016.

[10] **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. Progress in Cryptology an Information Security in Latin America. Revised Selected PapersLecture. Springer (2014). Diego F. Aranha, Alfred Menezes Eds. ISBN: 978-3-319-16294-2. ISSN: 0302-9743. ITEM:9783319162942. Disp en:http://rd.springer.com/chapter/10.1007% 2F978-3-319-16295-9_10.

[11] **PAAR C., PELZL J.:** "The One-Time Pad" - Chapert 2: Stream Ciphers in Understanding Cryptography Springer Berlin Heidelberg New York. ISBN 978-3-642-04100-6 e-ISBN 978-3-642-04101-3. DOI 10.1007/978-3-642-04101-3

[12] **GARCÍA P., BAST S., MONTEJANO G., 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.

[13] **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. Disponible en: http://conaiisi.unsl.edu.ar /2013/25-483-1-DR.pdf.

.