Avances en Aspectos de Seguridad en el Sistemas de Voto Electrónico OTP-Vote

Silvia Bast[1] Germán Montejano[2] MarioBerón[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
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, mberon]@unsl.edu.ar – web: http://www.unsl.edu.ar

RESUMEN

Los sistemas de voto electrónico no son ampliamente aceptados en la sociedad actual. Esta situación se debe principalmente a experiencias fallidas que han tenido lugar en elecciones recientes y conducen a que se acreciente la desconfianza de los electores.

En 2016 se presentaron las bases del sistema de votación denominado OTP Vote. El modelo usa múltiples claves One Time Pad que se combinan para formar una sola y son quienes dan el nombre al sistema. En este último tiempo se ha trabajado sobre el modelo original, con el objetivo de incrementar la confiabilidad e integridad del sistema en las diferentes etapas que incluye el proceso electoral. Las mejoras se orientan a: la configuración de los datos electorales y el proceso de generación y recuperación de votos, además de propuestas de auditoría y de verificabilidad end to end.

En este trabajo se exponen los avances que se llevaron a cabo para cada una de etapas del proceso.

Palabras clave: Sistemas de Voto Electrónico, Anonimato, Transparencia, Auditoría, One Time Pad, Verificabilidad End to End.

CONTEXTO

El presente trabajo surge de una de las líneas de investigación del proyecto "Aspectos de Seguridad en Proyectos de Software", que avanza en el desarrollo de un modelo de voto electrónico basado en criptografía one time pad. El proyecto de la Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa del (Resolución N° 488/14 del Consejo Directivo de la Facultad de Ciencias Exactas y Naturales) es dirigido por el Doctor Germán Antonio Montejano (Universidad Nacional de San Luis) y codirigido por el Magister Pablo Marcelo García (FCEyN - UNLPam) e incluyó como investigadores a la Magister Silvia Gabriela Bast, al Magister Daniel Vidoret, al Analista Programador Adrián García y al Programador Superior Claudio Ponzio.

El proyecto se desprendió de 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

Opiniones contrapuestas que van más allá del ámbito académico, se presentan en la sociedad actual respecto del tema voto electrónico. Quienes se oponen dudan acerca de la transparencia de los datos y presentan como pruebas excluyentes las experiencias fallidas que se han llevado a cabo con sistemas que no verifican los requisitos mínimos. Quienes están a favor, afirman en cambio que produce importantes mejoras en cuanto a precisión y rapidez en la divulgación de los resultados.

La opinión del equipo de trabajo es que, debido a que se trata de sistemas críticos, la confianza del electorado es el aspecto clave a tener en cuenta para lograr su aceptación. Así también lo afirman McGaley y Gibson [2] "Un sistema de votación es tan bueno como el público piensa que es".

Se asume también, que el sistema manual que se usa actualmente ofrece prestaciones aceptables. Sin embargo, si se tiene en cuenta que un amplio abanico de servicios sensibles y cotidianos se realizan virtualmente, se plantea el desafío de analizar y evaluar las condiciones de seguridad que deben cumplir los sistemas de voto electrónico y las soluciones propuestas por otros autores, con el objetivo de generar un modelo que permita el desarrollo de un sistema robusto y confiable.

En cuanto al concepto de Sistema de Voto Electrónico, Odrisek [3] afirma que es un componente de software que mapea electrónicamente el procedimiento de votación, para McGaley y Gibson [2] el voto electrónico es cualquier forma de recolección de votos que involucre dispositivos electrónicos (generalmente computadoras).

Epstein [4], Kazi, Alam y Tamura [5], Prince [6] y van de Graaf, Henrich y Müller-Quade [7], Hao, Ryan `[8], Rivest [9], Ryan P., Schneider S., Teague V.[10], Rabin M y , Rivest R [11] y Awad M. y Leiss E [12], se explayan sobre las características y los requisitos que deben cumplir estos sistemas y sobre antecedentes de los mismos.

En relación a la seguridad de los datos, los sistemas de votación electrónica deben proteger: el anonimato del elector por tiempo indefinido y los datos de los votos durante el proceso electoral, ya que luego la información se hace pública.

El Modelo OTP-Vote

El modelo OTP- Vote se describe en [13] se enfoca especialmente en la confidencialidad e integridad de los datos de un sistema de voto electrónico.

El modelo hace uso de los siguientes elementos de datos:

1. Claves One Time Pad (OTP), aleatorias y tan largas como el mensaje que cifran. Cumplen con las hipótesis y condiciones del "Secreto Perfecto" de Shannon [14].

2. Archivos de Datos que Almacenan Bits, son elementos centrales en el modelo propuesto y se van modificando durante el proceso.

   • Archivo Binario de Votos (ABV) surge en base al modelo de almacenamiento Múltiples Canales Dato Único (MCDU) propuesto por García en [15], que se analiza en profundidad en [16] y [17] y surge como una propuesta de resolución a las limitaciones de Birthday Paradox [18].

   • Clave de Descifrado (CD): se genera a partir de operaciones XOR (⊕) [19] de claves OTP.

3. Tablas del modelo relacional: mantienen los datos básicos de la configuración de la elección: cargos,

candidatos e identificadores de votos y de los votos planos resultantes del proceso eleccionario.

El modelo propone:
- Anonimato incondicional.
- Seguridad computacional que puede llevarse a cualquier nivel exigible durante el proceso eleccionario.

El proceso incluye las etapas de:
- Configuración de la elección que incluye:
  - La definición de las dimensiones de ABV y CD, configuración de los atributos de la tupla.
  - Generación de los códigos para cada uno de los atributos identificadores (Cargos, Candidatos e Identificadores de Votos).
  - Generación de las tablas: Identificadores de Votos, Cargos, Candidatos, con los identificadores producidos anteriormente.
  - La inicialización del ABV y la CD con la intervención de las autoridades electorales (CA), mediante el aporte de claves.
- Desarrollo de la elección que involucra:
  - Autenticación: consiste en verificar que el elector se encuentre registrado en el padrón de votantes.
  - Emisión del voto: una vez que el usuario es habilitado, pasa a elegir el candidato de su preferencia para cada cargo y emite su voto.
- Cierre de la elección y recuento de votos que incluye:
  - Inicio del proceso de descifrado mediante la intervención de las autoridades electorales con sus claves.
  - Obtención del archivo binario de votos descifrado.
  - Generación de la tabla de votos planos.

El modelo teórico presentado supone, para cada una de las etapas mencionadas, el cumplimiento de algunas condiciones que resultan imprescindibles para alcanzar el normal funcionamiento del sistema.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

Se trabaja en el mejoramiento del modelo original con el objetivo de convertirlo en un sistema de voto electrónico robusto, para ello, es necesario profundizar en aspectos de seguridad, tales como:

1. Uso de atributos de control, de encriptación y variaciones en la configuración de los datos de los votos.
2. Análisis y refinamiento de protocolos antifraude.
3. Análisis y selección de un método criptográfico que asegure la transmisión de datos entre estaciones y servidor.
4. Diseño de un modelo para la automatización del proceso de configuración de parámetros y generación de tablas relacionales del sistema de e-voting.
5. Análisis de la información intermedia que puede ser expuesta a los auditores para su control.
6. Verificabilidad End to End.

El modelo requiere entonces de la especificación de los puntos mencionados, para demostrar que el sistema resultante de la investigación es confiable y seguro.

3. RESULTADOS Y OBJETIVOS

Los avances en la investigación están dados por:

- Mejoras introducidas en las tres etapas del proceso en cuanto al uso de atributos de control y de encriptación, variaciones en la configuración de los datos en cada proceso eleccionario.
- Desarrollo del diseño de un modelo para la automatización del proceso de configuración de parámetros y generación de tablas relacionales del sistema de e-voting, que involucran la primera y última etapas del modelo.
- Análisis de las propuestas que se llevaron a cabo acerca de la información para el control de auditoría
- Avances en la propuesta de Verificabilidad End to End.

Como trabajo futuro, debe focalizarse en los siguientes aspectos:

- Análisis y refinamiento de protocolos antifraude en todas las etapas del modelo.
- Análisis y selección de un método criptográfico que asegure la transmisión de datos entre estaciones y servidor.
- La información intermedia que puede ser expuesta a los auditores para su control en la etapa de Desarrollo de la elección.
- Evaluación y profundización de los avances ya realizados sobre el modelo original.

4. FORMACIÓN DE RECURSOS HUMANOS

En cuanto a la formación de recursos humanos de esta línea de trabajo:

- Silvia Bast completó 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). Actualmente se encuentra desarrollando en su tesis doctoral Silvia Bast.

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", en Memorias del XV WICC. Ps 769-773. ISBN: 9789872817961. . 2013. .http://sedici.unlp.edu.ar/handle/10915/27537

[2] M. McGaley, J. Gibson, "A critical analysis of the council of Europe recommendations on e-voting". In EVT'06: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop. 2006.

[3] B. Odrisek, "E-Voting Security Study", Communications- Electronics Security Group, X/8833/4600/6/21, (Copyright The Crown) Issue 1.2 31 United Kingdom, 2002

[4] J. Epstein, "Electronic Voting" in Computer, vol. 40, no. 8, pp. 92-95, Aug 2007. doi: 10.1109/MC.2007.271.

[5] K. M. Rokibul Alam and S. Tamura, "Electronic voting - Scopes and limitations", International Conference on Informatics, Electronics & Vision (ICIEV), Dhaka, Bangladesh, pp. 525-529, . 2012. doi: 10.1109/ICIEV.2012.6317324.

[6] A. Prince, "Consideraciones, aportes y experiencias para el Voto electrónico en Argentina", Editorial Dunken, 2006.

[7] J.van de Graaf, C. Henrich, J. Müller-Quade, "Requirements for secure voting", Work Notes 2011.

[8] F. Hao, P. Ryan, "Real -World Electronic Voting. Design, Analysis and Deployment". CRC Press. ISBN-13: 978- 1498714693. ISBN-10: 1498714692. 2017.

[9] R. Rivest, "On the notion of 'software independence' in voting systems".

Philosophical Transactions of The Royal Society A, 366(1881):3759–3767. 2008.

[10] P. Ryan, S. Schneider, V. Teague, "End-to-End Verifiability in Voting Systems, from Theory to Practice". Voting Systems, from Theory to Practice. IEEE Security & Privacy, 13(3):59–62, 2015.

[11] M. Rabin, R. Rivest, "Efficient End to End Verifiable Electronic Voting Employing Split Value Representations" Bregenz, Austria. Proceedings of EVOTE 2014. ISBN 978-9949-23-688-6. 2014.

[12] M. Awad, E. Leiss, "End-to-End Cryptography: Spreading Democracy". International Journal of Applied Engineering Research. Volume 11, Issue 11. Ps. 7391-7394. 2016

[13] S. Bast, "Confidencialidad e Integridad de Datos en Sistemas de E-Voting – Un Modelo para la Implementación Segura de un sistema de Voto Presencial", Editorial Académica
Española. ISBN 978-3-639-53793-2. 2017.

[14] C. E. Shannon, "Communication theory of secrecy systems," in The Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x..

[15] P. García, "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.

[16] J. van de Graaf, G. Montejano, P. García, "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. 2013 Disponible en: http://42jaiio.sadio.org.ar/proceedings/simposios/Trabajos/WSegI/03.pdf.

[17] P. García, G. Montejano, S. Bast, E. Fritz, "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.

[18] P. García, J. van de Graaf, A. Hevia, A. Viola, "Beating the Birthday Paradox in Dining Cryptographers Networks". En "Progress in Cryptology – Latincrypt 2014". Springer International Publishing. ISSN: 0302-9743. ISSN (electrónico): 1611-3349. ISBN: 978-3-319-16294-2. ISBN (eBook): 978-3-319-16295-9. Ps. 179 – 198. Octubre, 2014.

[19] M. Murdocca, V. Heuring, "Principles of Computer Architecture. Appendix A: Digital Logic". Editor: Addison Wesley; Edición: US ed (29 de noviembre de 1999) Idioma: Inglés - ISBN-10: 0201436647 - ISBN-13: 978-0201436648