Requerimientos de Hardware y de Software en la Implementación de un Sistema de Voto Electrónico Distribuido

Pablo M. Davicino* Marcela Capobianco Alejandro G. Stankevicius

Laboratorio de Investigación en Sistemas Distribuidos
Departamento de Cs. e Ing. de la Computación
Universidad Nacional del Sur
Bahía Blanca - Buenos Aires - ARGENTINA
e-mail: {pmd, mc, ags}@cs.uns.edu.ar

Resumen

El objetivo central de esta línea de investigación consiste en analizar los requerimientos formales a nivel de hardware y de software que todo sistema de voto electrónico distribuido, actual o futuro, necesita demostrar que cumple a fin de preservar los derechos de los electores consagrados en el Código Electoral Nacional (Ley 19445), prestando particular atención al rol que desempeña la infraestructura de red y al uso que se le da a los servicios de encriptado y firma digital. En este sentido, en la actualidad no existe un conjunto uniforme de criterios a exigir a la hora de implementar este tipo de soluciones informáticas, como se evidencia a partir de los pobres resultados obtenidos en las distintas intentonas de adopción de tales mecanismos.

Palabras Clave: sistemas distribuidos, redes de computadoras, seguridad, privacidad

Contexto

La línea de investigación que estamos reseñando se encuentra en desarrollo en el seno del *Laboratorio de Investigación en Sistemas Distribuidos* (LISiDi), sito en el Departamento de Ciencias e Ingeniería de la Computación (DCIC) de la Universidad Nacional del Sur (UNS). El LISiDi cuenta con un importante número de estudiantes graduados con tesis doctorales y de maestría completas o en progreso, además de contar con oficinas y equipamiento informático de última generación, así como de un cluster propio de computadoras sobre una red ethernet de alta velocidad. Para esta primer etapa se optó por hacer uso de los fondos propios que la universidad destina a la investigación como fuente de financiación, habiéndose conformado un Proyecto Grupo de Investigación (PGI) a tal efecto, el cual se encuentra bajo el proceso de acreditación.

*Parcialmente financiado por la Comisión de Investigaciones Científicas de la Provincia de Buenos Aires.

Introducción

El análisis, diseño e implementación de sistemas resulta una tarea mucho más demandante de lo que *a priori* podría parecer. Nada sustenta esta opinión de manera más contundente que la denominada *crisis del software*, donde sistemas y soluciones informáticas que en abstracto parecen funcionar de manera aceptable, fracasan estrepitosamente al ser puestas en

funcionamiento a escala real. Todo parece indicar que pequeños descuidos en la especificación de los requerimientos formales, que ciertos malentendidos entre el personal a cargo del diseño de las distintas partes del sistema, y que alguna falta de comunicación entre los grupos de programadores a cargo de las distintas partes del proyecto, atentan al manifestarse en conjunto a la integridad del sistema como un todo. Si bien cada uno de estos cuestionamientos son seguramente fáciles y simples de detectar y corregir por separado, al confluir terminan provocando no solo demoras en el cumplimiento de los plazos pactados, sino también un deterioro en la calidad del producto resultante.

El sistema actualmente en uso a la hora de llevar adelante una elección general, aquel que depende de engorrosos padrones impresos en papel, urnas de madera o más recientemente de cartón y una infinidad de boletas para los distintos partidos políticos participantes, el cual más aun gira en torno a un lento y tedioso proceso de escrutinio manual, constituye un marco ideal en el cual ensayar una solución superadora basada en un sistema autónomo y automático que haga uso de una red de computadoras. No obstante, si tenemos en cuentas las características de este escenario caeremos en cuenta de que también constituye un ejemplo de libro de texto de un sistema dónde la crisis del software ha de expresarse con mayor fuerza.

Cabe señalar en este punto que Argentina ha ensayado en la última década distintas implementaciones tentativas de sistemas de voto electrónico de la más variada naturaleza pero con un factor constante: los paupérrimos resultados obtenidos al intentar hacer uso de los mismos en una elección no virtual. La tan publicitada fase de adopción masiva de estos sistemas nunca se concretó, considerando que los resultados obtenidos en la práctica usualmente diferían de los objetivos pautados antes de su implementación. Mantener al mismo tiempo *la privacidad* y *la integridad* de los votos constituye metas encontradas a la hora de implementar un sistema de software; no hay manera de resolver esta problemáticas sin hacer de uso de avanzadas técnicas de firma digital y encriptado asimétrico de datos, junto con la no trivial infraestructura pública que la aplicación satisfactoria de estas técnicas requieren.

En este sentido, consideramos que las investigaciones enmarcadas en la presente línea tienen el potencial de tener un impacto considerable en la sociedad en caso de continuarse con la tendencia actual de impulsar la reimplementación del sistema actual en términos de una solución informática, según se desprende de las manifestaciones públicas de los principales referentes de los distintos partidos políticos.

Finalmente, cabe acotar que en la actualidad *no existe un conjunto uniforme de criterios* a exigir a la hora de implementar este tipo de sistemas, ya que la crítica a las falencias de los mismos suelen estar centradas en cuestiones no tan técnicas, si bien no por ello menos trascendentes, tales como el costo de implementación de la solución informática o lo complejo de asegurar el acceso a la energía eléctrica en todos los recintos de votación del país.

Líneas de investigación y desarrollo

La presente línea de investigación tiene como finalidad específica analizar los requerimientos formales a nivel de hardware y de software que todo sistema de voto electrónico distribuido, actual o futuro, necesita demostrar que cumple a fin de preservar los derechos de los electores consagrados en los artículos del Código Electoral Nacional (Ley 19445), prestando particular atención al rol que desempeña la infraestructura de red y al uso que se le da a los servicios de encriptado y firma digital.

Este conjunto de requisitos juega un doble papel, por un lado sirve como marco de referen-

cia contra el cual contrastar todo nuevo sistema, a fin de verificar si el mismo estará en condiciones de preservar los derechos de los electores. Asímismo, también sirve como andamiaje inicial de todo nuevo proyecto de desarrollo de tal sistema. Si los requisitos identificados como producto de estas investigaciones son tenidos en cuenta desde el comienzo del análisis y diseño de un nuevo sistema, el producto obtenido al final del proceso de desarrollo seguramente resultará más robusto y acorde a los objetivos deseados.

Resultados y objetivos

El propósito de las investigaciones enmarcadas en la presente línea es perfeccionar el estado del arte en lo que al diseño, implementación y evaluación de sistemas de voto electrónico distribuido concierne. A su vez, estas investigación también servirán de marco para la formación de recursos humanos a través del desarrollo de tesis de grado y/o de posgrado en el área.

Nos proponemos satisfacer este objetivo general a través de la prosecución de los siguientes objetivos específicos:

1. Tomar contacto con el estado del arte en la materia a partir de una acabada la revisión bibliográfica.

2. Estudiar las características particulares de las soluciones de software y hardware preexistentes, hasta donde las respectivas licencias lo permitan.

3. De este análisis preliminar, identificar un conjunto extendido de requerimientos razonables de software y de hardware.

4. Estudiar el conjunto extendido de requerimientos a fin de proponer un conjunto representativo de éstos.

5. Validar el conjunto propuesto de requerimientos de software y hardware contra las soluciones preexistentes, a fin de determinar cuáles se verifican y cuáles no.

Naturalmente, también constituye un objetivo tácito la publicación en congresos y revistas del área de tanto los resultados parciales como los resultados finales que se produzcan a lo largo de esta investigación.

Formación de recursos humanos

Esta línea de trabajo tiene el potencial de desempeñar un importante rol en la misión educativa de nuestra unidad académica. Las tareas asociadas al desarrollo de esta línea de investigación contribuyen a la formación de estudiantes de grado y posgrado y las mismas están integradas en el programa de materias del Departamento de Ciencias e Ingeniería de la Computación. Se anticipa que varios estudiantes de grado y posgrado, y en particular becarios, se sumen a lo largo de su desarrollo.

Bibliografía

Unos de los aspectos más interesantes de cotejar distintas líneas de investigación consiste en estudiar y analizar las citas bibliografícas reseñadas. En este sentido, en primer lugar hemos de citar la bibliografía estrictamente pertinente a los sistemas de voto electrónico directo, también conocidos como sistemas DRE (*Direct Recording Electronic voting system*):

- Busaniche, B., and Heiz, F. *Voto electrónico - Los Riesgos de una Ilusión.* Fundación Via Libre, 2008.

- Harris, B. *Black Box Voting: Ballot Tampering in the 21st Century.* Talion Publishing, 2004.

- Prince, A. *Consideraciones, aportes y experiencias para el voto electrónico en Argentina*. Editorial Dunken, 2006.

A continuación sintetizamos el material en relación a las restantes disciplinas que cubren el tópico central como ser *sistemas distribuidos*, *redes de computadoras*, *ingeniería de software* y *seguridad en sistemas*:

- The ISO/IEC 27000 series standard for IT security evaluation. `http://www.iso27001security.com`.
- Abrams, M. D., Sushil, J., and Podell, H. J. *Information Security: An Integrated Collection of Essays*. Institute of Electrical & Electronics Engineer, 1994.
- Ahuja, V. *Network and Internet Security*. Academic Press, 1996.
- Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley, 2008.
- Dollimore, J., Kindberg, T., and Coulouris, G. *Distributed Systems: Concepts and Design*, 4th ed. Addison-Wesley, 2005.
- Flegel, U. *Privacy-Respecting Intrusion Detection*. Springer, 2010.
- Foster, I. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. *International Journal of Supercomputer Applications 15*, 3 (2001), 200–222.
- Foster, I. What is the Grid? A Three Point Checklist. *GRIDToday 1*, 6 (2002), 32–36.
- Glass, G. *Web Services: Building Blocks for Distributed Systems*. Prentice Hall PTR, 2001.
- Gollmann, D. *Computer Security*, 3rd ed. Wiley, 2011.
- Kaufman, C., Perlman, R., and Speciner, M. *Network Security: Private Communications in a Public World*, 2nd ed. Prentice Hall, 2002.
- Koblitz, N. *A Course in Number Theory and Cryptography*, 2nd ed. Springer, 1994.
- Kurose, J. F., and Ross, K. W. *Computer Networking - A Top-Down Approach Featuring the Internet*, 5th ed. Addison Wesley, 2009.
- Leopold, C. *Parallel and Distributed Computing: A Survey of Models, Paradigms and Approaches*. Wiley-Interscience, 2000.
- Luby, M. G. *Pseudorandomness and Cryptographic Applications*. Princeton University Press, 1996.
- MacGregor, R. S., Aresi, A., and Siegert, A. *WWW Security: How to Build a Secure World Wide Web Connection*. Prentice Hall, 1996.
- Northcutt, S., and Novak, J. *Network Intrusion Detection*, 3rd ed. Sams, 2002.
- Rivest, R. L., Shamir, A., and Adleman, L. M. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM 21*, 2 (1978), 120–126.
- Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. Wiley, 1996.
- Silberschatz, A., Galvin, P. B., and Gagne, G. *Operating Systems Concepts*, 8th ed. Wiley, 2008.

- Summers, R. C. *Secure Computing: Threats and Safeguards*. Mcgraw-Hill College, 2000.
- Tanenbaum, A. S. *Modern Operating Systems*, 3rd ed. Prentice Hall, 2007.
- Tanenbaum, A. S., and Steen, M. V. *Distributed Systems: Principles and Paradigms*, 2nd ed. Prentice Hall, 2008.
- Tanenbaum, A. S., and Wetherall, D. J. *Computer Networks*, 5th ed. Prentice Hall, 2010.