FACULTAD DE CIENCIAS EXACTAS Y NATURALES
Universidad Nacional de La Pampa

FACULTAD DE CIENCIAS FÍSICO MATEMÁTICAS Y NATURALES
Universidad Nacional de San Luis

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

Silvia **BAST**, Germán **MONTEJANO**, Mario **BERÓN**

Resumen

Los sistemas de voto electrónico son sistemas de seguridad crítica y no cuentan con amplia aceptación en la sociedad actual debido, principalmente, a experiencias fallidas que 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. Se han desarrollado mejoras al modelo original, con el objetivo de incrementar la confiabilidad e integridad del sistema. Los avances se enfocan en: la configuración de los datos electorales y el proceso de generación y recuperación de votos, propuestas de auditoría y de verificabilidad end to end.

Contexto

El trabajo surge como una línea de investigación del proyecto "Aspectos de Seguridad en Proyectos de Software" (Facultad de Ciencias Exactas y Naturales de la Universidad Nacional de La Pampa), que avanza en el desarrollo de un modelo de voto electrónico basado en criptografía one time pad.

Formación de Recursos Humanos

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.

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, 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 del modelo relacional 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

Avances

- Mejoras introducidas en las tres etapas del proceso en cuanto al uso de atributos de control y de encriptación y variaciones en la configuración de los datos en cada etapa del 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.

CONTACTO

silviabast@exactas.unlpam.edu.ar
gmonte@unsl.edu.ar
mberon@unsl.edu.ar

RedUNCI - UNdeC. ISBN 978-987-24611-4-0