

[Tendencias y Desafíos en Seguridad Computacional]

Alejandro Hevia
CLCERT & Dept. Cs. Computación
U. Chile

[Temas País]

- Votación electrónica
- El valor de la privacidad

[Votación Electrónica]

*O como convencer a los que
perdieron que perdieron
(electrónicamente)*

[D. Wallace]

[Antecedentes: Votación Clásica de lápiz y papel]

- Corto historial (1958) pero conocido
- Criterios usuales para evaluarlo
 - Robustez / confiabilidad del sistema,
 - Posibilidad de error por parte del votante,
 - Usabilidad,
 - Costo.

[Sistema de Votación Actual]

- Mejorable?
 - Tema sensible...
Investigación académica vista como cuestionamiento a políticos.
- *Un sistema nuevo debe ser al menos tan bueno como el sistema que reemplaza.*

[Votación Electrónica: La Idea]

- Máquina de votación
 - tipo cajero automático
 - Pantalla sensible al tacto, o botones
- Reporte y tabulación electrónica de resultados



Beneficios de la Votación Electrónica

Usualmente mencionados:

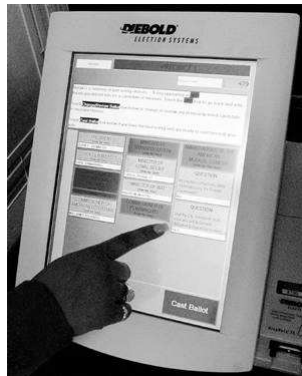
- Costo, rapidez (aumentar frecuencia)
- Reducir fraude y abuso
- Aumentar participación ciudadana
- Preguntas complejas o múltiples
- Diferentes lenguajes (mapudungun)
- “Imagen de Modernidad”

Votación Electrónica en el mundo

- | | |
|--------------|-------------------|
| ■ EEUU | ■ Holanda |
| ■ Inglaterra | ■ Irlanda |
| ■ Estonia | ■ India |
| ■ Brazil | ■ Alemania |
| ■ Suiza | ■ Kazakhstan |
| ■ Italia | ■ ... entre otros |

No todos los intentos han sido exitosos...

[Problema no es tan fácil]



≠



[Votación-E ≠ Cajero-E]

- Tipo de bien transado (comprado) es distinto
 - quien provee el servicio no es pagado por quien compra:
 - ¿cuánto vale ganar una elección?
- Auditar no es simple! Anonimato no puede violarse

Objetivos de un sistema de Votación Electrónica

- “Debe convencer a los perdedores que perdieron”
 - Perdedor sin conocimiento técnico
 - Potencialmente bajo el control de uno de los candidatos

Objetivos de un sistema de Votación Electrónica

- **Correcto:** intención de voto plasmada en el total
 - No se puede cambiar el voto de otro, agregar votos ilegítimos, destruir votos (o afectar correctitud del cómputo)
- **Privacidad del voto** (Anonimato)
- Sistema **escalable:**
 - millones de usuarios, varias preguntas
- **Fácil** de usar, administrar

[Problemas Inherentes]

- Votante no ve representación del voto
- Voto almacenado en memoria del computador, fuera de la vista del votante
- Computador hace lo que dice... O no?
- Computadores tienen errores... (ineludible debido a complejidad)
 - Problema si errores NO son aleatorios

[Más Problemas Inherentes]

- Potencial de modificación no autorizada invisible y/o "Hackeo"
 - Externo (gran motivación, gobierno extranjero?)
 - Interno (desarrollador, operador, atacante infiltrado)
 - Error puede afectar a miles de maquinas
- Vendedor: Ok si no se detectó problema...
 - Falso: No detección ≠ No hay problema

[Problemas Reales]

- 2001: Volusia county, Florida, EEUU:
 - Al Gore obtiene -16022 votos en una mesa
- 2003: Boone county, Indiana: 140 mil votos en área con 6000 votantes inscritos
- 2006: Sarasota, Florida, EEUU: en por elección ganada por 386 votos de un total de 153 mil, 13% votantes parecen no votar
- Cientos de otros casos documentados (en EEUU y otros países)

[Para tener en mente...]

- *“No es quien vota el que cuenta, si no quien cuenta los votos.”*

[Atribuido a J. Stalin]

[Votación Electrónica: el desafío (parte 1)]

- **Exactitud:** resultado final debe reflejar las intenciones del votante
 - A lo más un voto por cada votante autorizado
 - Voto emitido según preferencia
 - Voto contado tal cual como fue emitido
 - Disponibilidad del sistema
- **Privacidad:** Nada revelado de un voto individual excepto el cómputo final

[Votación Electrónica: el desafío (parte 2)]

- **Proceso y resultado verificable**
 - Voto fue contado
 - Resultado es correcto
 - Verificación por votantes y/o terceros
- **No hay recibo**
 - Votante no puede probar cómo votó, aún si quiere
 - Evita compra de votos y coerción

[Pero es posible: Recomendaciones]

- Sistema debe ser **redundante**
 - Copia en papel del voto por si recuento manual
- **Auditable**: verificación abierta, profesional
 - Software satisface especificación (lo más simple posible!), revelar código ayuda
 - Siempre considerar ataques internos y externos
 - Certificación por entidades públicas, con código disponible (al menos componentes críticas)

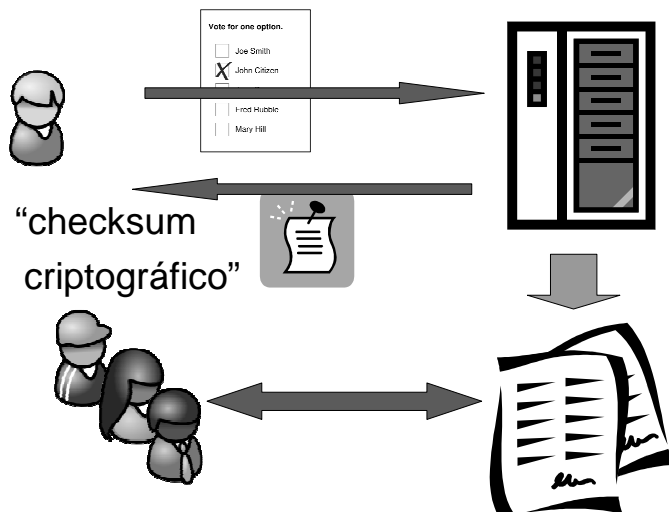
[Más recomendaciones]

- Autenticación de software / hardware
 - ¿Cómo saber que el software que certificamos corre en una máquina? (attestation, criptografía)
- Transporte seguro de equipos
- Registros de la elección deben ser públicos
- Procedimientos claros de evaluación / certificación / reportes en caso de fallas
 - Fallas son investigadas, resultados públicos, estándares re-evaluados
 - Emular caso: aviones, tragamonedas en casinos

Evitando el peor caso:
Registro en papel



Verificación de operación
correcta *durante* votación



[Votación por Internet?]

- Ambiente NO controlado



No: Coerción, malware

- Ambiente controlado



Si: Recinto satélite

[Conclusiones y otros desafíos]

- Votación electrónica requiere planificación, definir estándares
- No basta comprar “paquete armado”
- Remota, ambiente no controlado: NO!

- Otro desafío:
Registro electoral electrónico / online
[Piquer-Poblete 2005]

[El Valor de la Privacidad]

[Dos tendencias hoy]

- Costumbre Chilena usual de “entregar nuestros datos” (RUT, dirección, etc.)
- Perseguir más duramente a delincuentes, monitorearlos e identificarlos.

Efecto combinado?

[Minería de Datos: mejor que extraer cobre?]

- Enormes bases de datos con información de cada uno de nosotros
 - Si, útiles para algunas aplicaciones (ej. policial, seguridad nacional)
 - Pero también otros fines – comerciales.

[¿Qué es la Privacidad?]

- “*¿Si no haces nada malo, que tienes que ocultar?*”
 - Asume que privacidad es ocultar algo malo
- La privacidad es un derecho humano
 - Derecho a ser dejado tranquilo
 - En mi baño, en mi cama, al opinar en privado, al cantar en la ducha

[El problema no es nuevo]

- *“¿Quién observa a los observadores?”*
[Proverbio]
- *“El poder absoluto corrompe absolutamente.”*
[Proverbio]

[Privacidad vs. Supervigilancia]

- *“Si me dieran seis líneas escritas por el hombre más honesto de todos, encontraría algo en ellas para mandarlo a la horca.”*
[Cardenal Richelieu]
- *“Mira a alguien lo suficiente y seguro tendrás algo por lo cual arrestarlo o con lo cual extorsionarlo.”*
[Bruce Schneier]

[Privacidad: Incentivos en contra]

- Entregamos nuestros datos por
 - Conveniencia (tarjeta crédito)
 - Descuentos (tiendas)
 - Comodidad (trámites)
 - Cuenta de correo / página web gratis
 - Popularidad (redes sociales)

[Erosión progresiva de privacidad]

- No un sólo “*big brother*” si no miles de pequeños “*little brothers*”
 - Google, MySpace, facebook
 - VoIP (voz sobre IP)
 - Tiendas comerciales, gobierno
- Tentación usual es sobre-extenderse en leyes de retención de datos

[¿Conviene amasar datos?]

- Pareciera, desde un punto de vista económico
- **Liability**: Esta información debe ser protegida
 - Protección tiene un costo
 - Ataques internos son muy comunes
- Menos que guardar, menos que proteger

[Información vs. Privacidad]

- Es posible tener ambos
- Información ≠ datos
- Por ej. base de datos encriptada
 - Clave distribuida, NO disponible a un solo operario
 - Existen algoritmos para operar la BD, preguntar y responder!
 - Robar la BD ya no es tan útil

[Otros beneficios]

- Incluso **anonimato** es útil
 - Reportar crímenes, corrupción
 - Preguntar por enfermedades de carácter “humillante” o posiblemente discriminantes (Sida, cáncer, etc.)
 - Evaluar opinión real de la ciudadanía

[Hacia una estrategia de solución]

- Leyes que regulen la creación, uso, protección, reventa y eliminación de los datos personales
- Uso de estándares para definición e intercambio de políticas de privacidad
- No pedir / entregar datos “extras” cuando se requiere sólo uno particular.

[Conclusiones]

- Preservar privacidad no solo por “libertad” sino para evitar filtraciones catastróficas y disminuir costos!
- Existen alternativas tecnológicas (criptográficas) que permite establecer y manejar balance.