Voto telemático y voto electrónico

Criptografía y Computación

Marco Manuel Fernández Pranno
Granada, 2017.

Índice

1. Características de un sistema de voto

- **Precisión**: Establecer la intención de cada votante y representarlo en un resultado final. No siendo posible la alteración de los votos por una entidad ajena.
- **Anonimato**: Imposible identificar al individuo votante durante el proceso.
- **Escalabilidad**: Capaz de manejar cargas de trabajo muy grandes. (Ej: 372 millones en India, 115 millones en Brasil)
- **Velocidad**: Presentar un resultado final con presteza (pocas).

2. Mejoras respecto al sistema convencional

- En ciertos sistemas, más conveniente para los votantes ya que no hay necesidad de traslado.
- Más eficientes y menos recursos (tanto humanos como materiales)
- Ofrecen enormes ventajas frente al uso de distintos idiomas o votantes con discapacidad.
- Tasa de error menor frente a sistemas convencionales, el error humano supera el error de un sistema electrónico.
- Mayor velocidad en el recuento.
- Con un diseño adecuado ofrece posibilidades de un análisis forense fiable para validar los resultados.

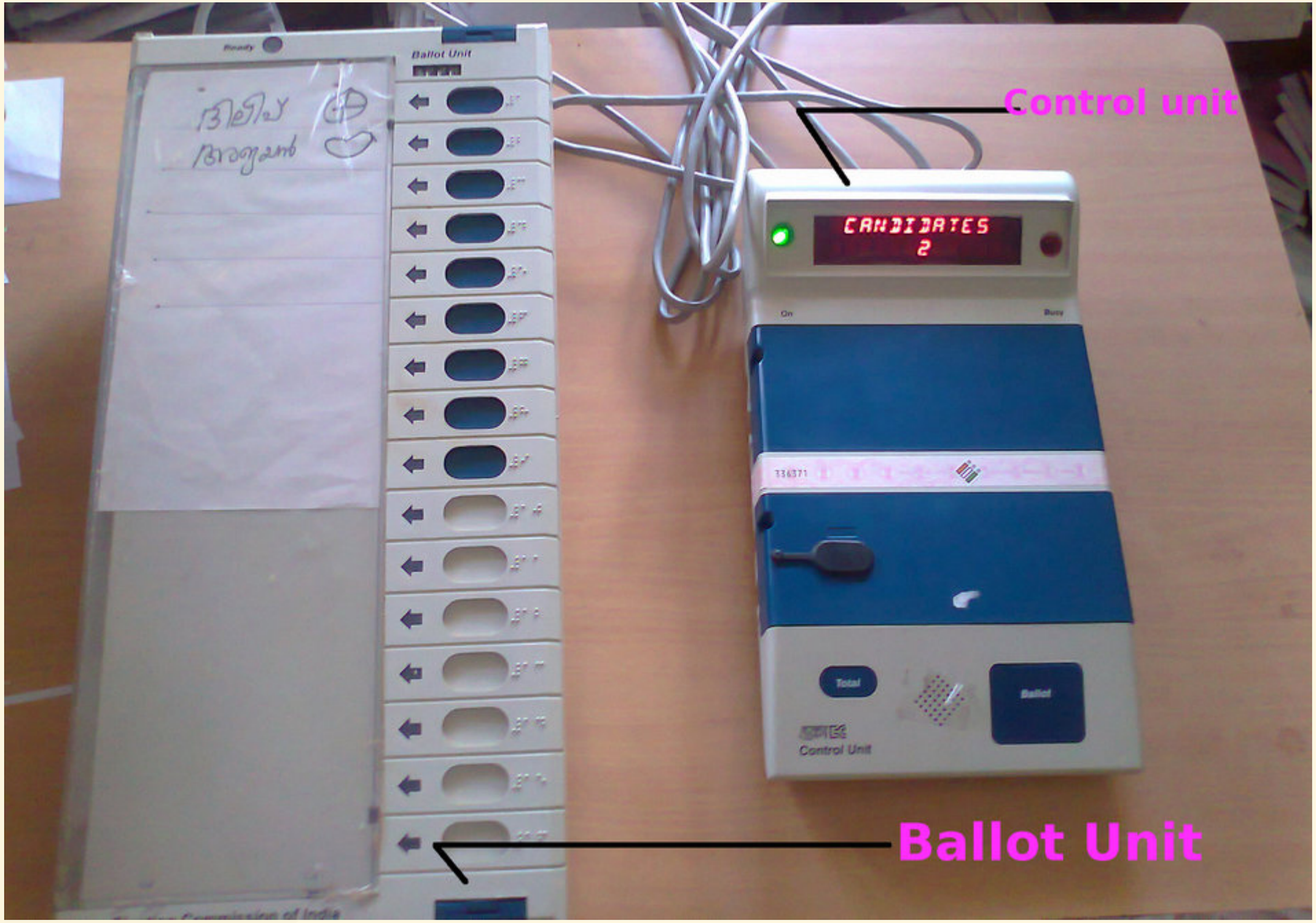
3. Precauciones, consideraciones y peligros

- Los errores no son uniformes, pueden favorecer/perjudicar a una opción particular.
- Pueden alterar las tasas de voto debido a la barrera de la tecnologica.
- Un error de software al ser explotado puede suponer la alteración de todo el sistema al completo.
- Extremadamente difíciles de testear en un ambiente real.
- Amenazas: Individuos, crimen organizado y agencias de inteligencia gubernamentales.

4. Situación actual

Direct Record Electronic (DRE): Sistema más extendido, una máquina física con interfaz de botones o táctil que ofrece las distintas opciones de voto.


JUSTIÇA
ELEITORAL
Lei nº 10.826, de 22/12/2003
O comércio de armas de fogo e munição deve ser proibido no Brasil?
1 - SIM
2 - NÃO
1 2 3
4 5 6
7 8 9
0
BRANCO
CORRIGE
CONFIRMA
PROCOMP


Control unit
CANDIDATES
2
Ballot Unit
Total
Ballot
Control Unit

DRE

- Información almacenada en una memoria extraíble, transportada a un lugar seguro para el recuento
- Verificación del voto con un impreso en papel, almacenado para casos de segundos recuentos y como medida de seguridad
- La mayoría ofrecen un feedback inmediato para verificar el voto correcto
- Generalmente software privativo
- La interfaz táctil da lugar a errores en el uso
- Suponen una inversión considerable, su mantenimiento y actualización no siempre es el óptimo

Ejemplo: Sequoia AVC Edge

Proceso de voto:

1. Tarjeta electrónica.
2. Selección de lenguaje y opciones.
3. Reconocimiento y almacenamiento del voto.
4. Reinicio de la tarjeta para asegurar solo un voto por votante.
5. Opcional: Se imprime un comprobante de la operación.

Ejemplo: Sequoia AVC Edge

Vulnerabilidades:

- Criptografía fácil de evadir
- Algoritmos de cifrado mal implementados
- Uso de algoritmos débiles con vulnerabilidades conocidas
- Todas las llaves de cifrado hardcodeadas en el sistema, idénticas en todos los sistemas.
  Lo que implica que alguien con acceso temporal a una máquina puede comprometer todos los sistemas de voto del país.

5. Posibles mejoras

- **Simplicidad**: Diseño sencillo y testeado
- **Uniformidad**: Sistema estandarizado en todos los puestos de voto
- **Verificabilidad**: Impresión de un certificado del voto, con validez para recuento y analisis posterior
- **Transparencia**: Codigo de dominio público, sujeto a escrutinio. Permitiendo una mejora y un análisis continuo del sistema

6. Futuro: Blockchain al rescate (?)

PRO:

- Sistema descentralizado
- Difícil modificación de los datos introducidos

CON:

- Votos almacenados permanentemente en la blockchain, de ser posible identificar a los votantes estos perderían el valor fundamental del voto anónimo/privado y los podría poner en grave peligro
- El resto de aspectos del sistema sigue siendo igual de vulnerable

7. Conclusión

Las mejoras respecto a los sistemas convencionales son indiscutibles, pero es de importancia crítica ser impecables en el diseño y mantenimiento de los mismos para que estén a la altura de la importancia de su tarea.

Establecer estándares facilitara el camino a la adopción unánime de unos sistemas robustos y fiables.

La auditoría pública tanto del software como el hardware, la existencia de métodos de análisis forenses posteriores y la existencia de un soporte físico con el que verificar los resultados son pilares fundamentales.

8. Bibliografía

- Bruce Schneier: The Problem with Electronic Voting Machines
- Bruce Schneier: American Elections Will Be Hacked
- Bruce Schneier: Why is it so hard to run an honest election?
- Ars Technica: Meet the e-voting machine so easy to hack, it will take your breath away
- Computerphile: Why Electronic Voting is a BAD Idea
- E-Voting Machine: Sequoia AVC Edge

8. Bibliografía

- Blockchain Technology in Online Voting
- Will Blockchain-Based Election Systems Make E-Voting Possible?
- Elon Musk: Mars government
- Patent: Electric voting-machine (1897)
- Wiki: Electronic voting
- Wiki: Certification of voting machines
- Wiki: E-Democracy
- Wiki: DRE voting machine

8. Bibliografía

- Block The Vote: Could Blockchain Technology Cybersecure Elections?
- Can the blockchain make electronic voting more secure?

8. Nota final

- MARP
- https://github.com/MarFerPra/electronic-voting