¿Exige la sociedad-red una nueva democracia?

Exigencias técnicas del voto electrónico

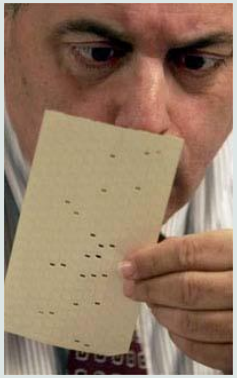
Definición

Utilización de tecnología de la información y las comunicaciones en todo el proceso electoral, o en algunas de las distintas fases del mismo.

Clasificación de los sistemas de votación

Clásico

- Votación mediante papeleta
- Maquina de palanca
- Tarjeta perforada
- Lector óptico



Clasificación de los sistemas de votación

Clásico

- Votación mediante papeleta
- Maquina de palanca
- Tarjeta perforada
- Lector óptico

Electrónico

- Urna electrónica: Demotek
- Equipos de registro electrónico directo (RED)

Sistemas electrónicos de votación

Los defensores de los sistemas electrónicos de votación señalan una serie de ventajas:

- Disminuyen las posibilidades de fraude electoral
- Su implementación aumenta la participación electoral
- Ahorro de costes
- Aumento de la velocidad en la presentación de los resultados
- Mejora de la precisión de los resultados
- Incrementa la accesibilidad para discapacitados
- Mayor flexibilidad
- Se podrían eliminar varios materiales electorales, como las papeletas.
- Son una consecuencia natural de la modernización

Sistemas electrónicos de votación

Alemania
Austria
Bélgica
Escocia
España
Francia
Holanda
Irlanda
Italia
…..

Brasil
Canadá
EE.UU.
México
Venezuela
…..

India Australia ……

Bélgica

- Introdujo el voto electrónico en 1991 para resolver los problemas derivados de la complejidad de su sistema electoral.

- Emplean el sistema Digivote desarrollado por Steria.

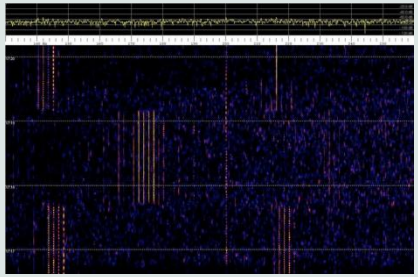
Holanda

- Nedap ES3B (2006)

- Expertos holandeses demuestran que el sistema podía ser fácilmente intervenido y se podían alterar los resultados electorales y desvelar el secreto del voto. *(http://www.wijvertrouwenstemcomputersniet.nl)*

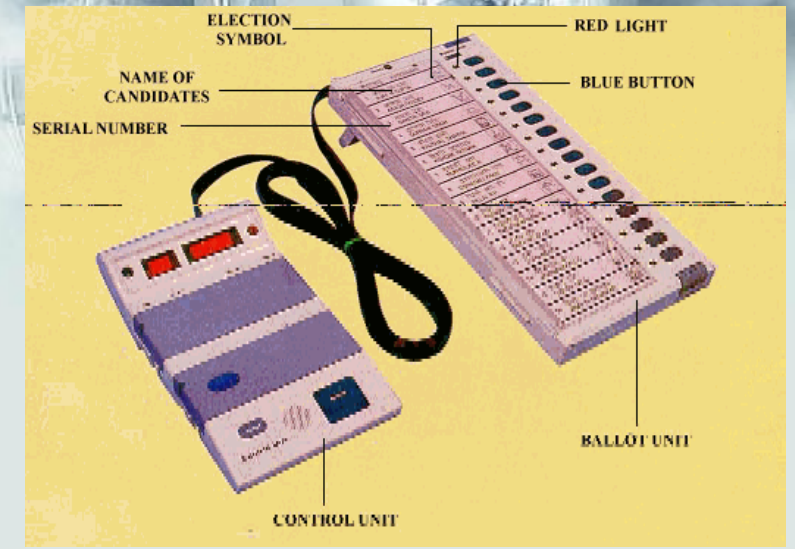
- El 1 de octubre de 2007, la Corte de Alkmaar en Holanda anulo la certificación de las máquinas de votación NEDAP

- Y no se usarán máquinas de votar en los próximos procesos electorales



India

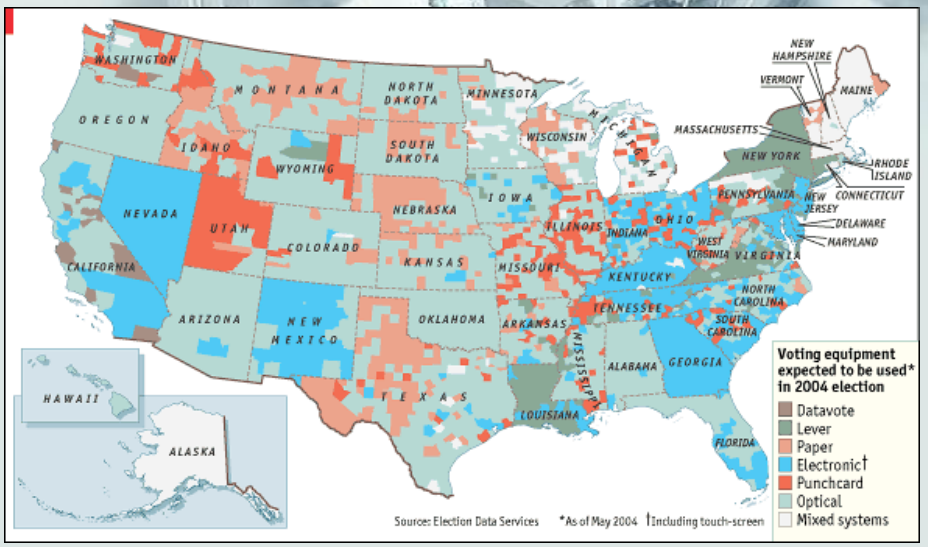
- En 1989 se puso en marcha el voto electrónico, aumentándose desde entonces de forma gradual el número de maquinas.
- En 2004 (Elecciones al Parlamento indio): Mas de un millón de maquinas electrónicas distribuidas en 700.000 colegios electorales de 543 distritos.
- 675 millones de electores. Se presentaron casi 800 partidos, miles de agrupaciones electorales y miles de candidatos independientes.
- Las maquinas de votar electrónicas fueron suministradas por dos empresas del país, con un coste reducido y un manejo simple.



Estados Unidos

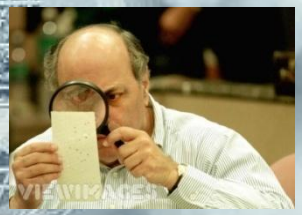
- Los Estados Unidos tienen un sistema electoral complejo en el que cada Estado e incluso cada Condado determina la forma y los recursos electorales a utilizar.

- En el año 2.004, la mayor parte de los votantes emplearon sistemas automatizados; 13,7% empleó tarjetas perforadas; 14% empleó sistemas de palanca; 34,9% lectura óptica y 29,3% empleó equipos DRE .



Estados Unidos

Escándalo en dos condados de Florida a causa de las tarjetas perforadas



13/09/2006: La Universidad de Princeton hace público un estudio sobre la seguridad de la máquina Diebold AccuVote-TS. El documento concluye que la máquina es vulnerable a varios ataques extremadamente serios, que minan la precisión y la credibilidad de los recuentos de votos con ella realizados.

27/7/2007: En un informe de la Universidad de Berkeley -California-, se llega a la conclusión de que las máquinas de votación (Diebold Election Systems Inc.) de la empresa Diebold no son lo bastante seguras para garantizar una elección fiable, y que el ataque de virus podría, a través de una sola máquina, interrumpir o cambiar el resultado de las elecciones.

7/12/2007: Universidad de Pensilvania: El informe EVEREST (Evaluation and Validation of Election-Related Equipment, Standards and Testing), que estudia sistemas de votación electrónicos de las empresas “Election Systems and Software (ES&S)” y “Hart InterCivic and Premier Election Solutions” (el 80% del voto en Estados Unidos). Se han detectado fallos de todo tipo, como por ejemplo, fallos debidos a “buffer overflows”, cifrado insuficiente (inexistente en algunos casos) y fallos de firmware, que posibilitan alterar el resultado de unas elecciones.

Estados Unidos

Dr. Aviel D. Rubin (director técnico del Instituto para Seguridad Informática de la Universidad John Hopkins):

“ Imagine por un momento que usted vive en un país donde nadie está seguro de cómo se cuentan los votos y no existen registros fiables para realizar un recuento. Imagine que las máquinas cuentan los votos pero nadie sabe como lo hacen. Ahora imagine que alguien descubre que estas máquinas son vulnerables a ataques, pero las agencias responsables no toman las medidas necesarias para hacerlas seguras. Si usted vive en U.S.A. no necesita imaginárselo. Esta es la realidad del voto electrónico en este país”.

(www.bravenewballot.org)

Clasificación de los sistemas de votación

Clásico

- Votación mediante papeleta
- Maquina de palanca
- Tarjeta perforada
- Lector óptico

Electrónico

- Urna electrónica: Demotek
- Equipos de registro electrónico directo (RED)

Telemático

- Centros de votaciones interconectados
- Votación desde “casa” a través de Internet

Voto telemático

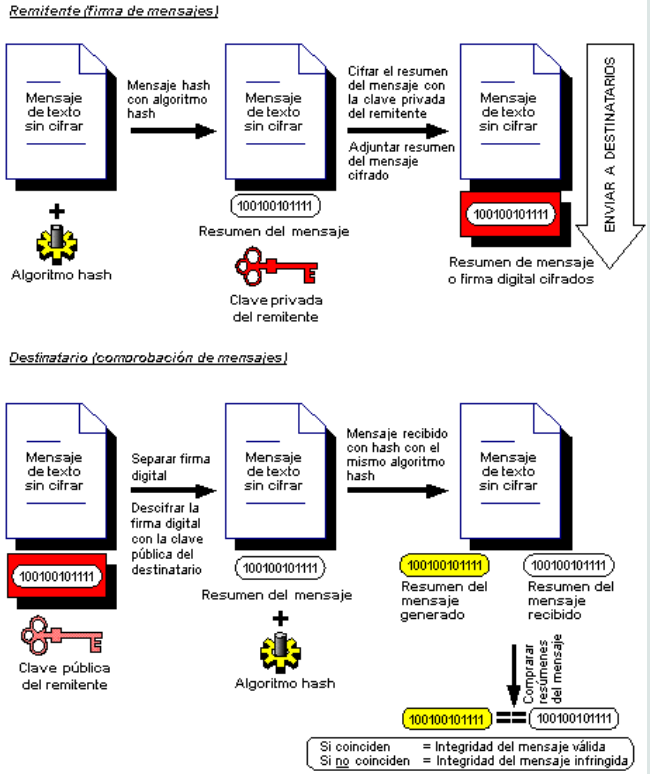
- Requisitos básicos de seguridad:
  - Identificación o autenticación
  - Confidencialidad de los datos
  - Integridad de los datos
  - Unicidad
  - Anonimato
  - Verificabilidad individual

Criptografía

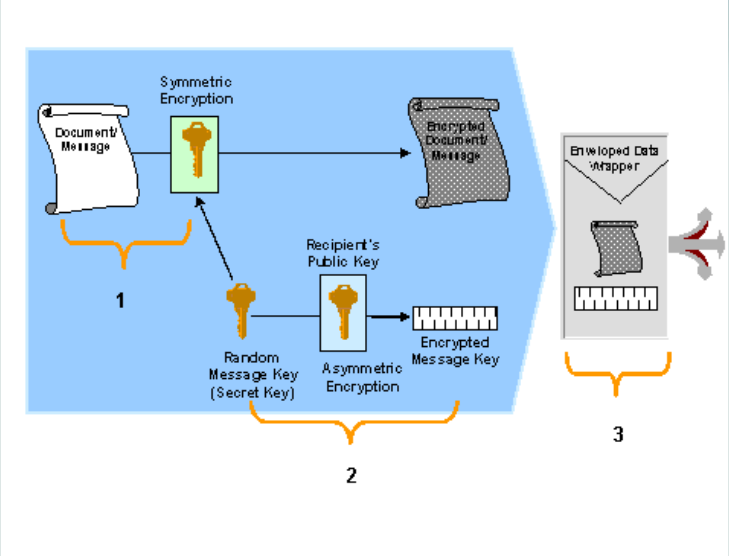
Criptografía

Clasificación:

- Criptografía clásica o simétrica
- Criptografía moderna, asimétrica o de clave publica



Firma electrónica



Sobre digital

Firma ciega

Voto telemático

- Requisitos básicos de seguridad:
  - Identificación o autenticación
  - Confidencialidad de los datos
  - Integridad de los datos
  - Unicidad
  - Anonimato
  - Verificabilidad individual

- Problemas derivados del uso de Internet
  - Ataques debidos al protocolo TCP/IP
  - Compra de votos
  - Acceso limitado a Internet
  - El ordenador del votante esta comprometido

Voto telemático

- Requisitos básicos de seguridad:
  - Identificación o autenticación
  - Confidencialidad de los datos
  - Integridad de los datos
  - Unicidad
  - Anonimato
  - Verificabilidad individual

- Problemas derivados del uso de Internet
  - Ataques debidos al protocolo TCP/IP
  - Compra de votos
  - Acceso limitado a Internet
  - El ordenador del votante esta comprometido

- Ventajas del voto telemático:
  - Movilidad y comodidad del votante
  - Los equipos se pueden utilizar en otras consultas y no sólo para las elecciones (democracia directa)

Conclusiones

1) El sistema de votación electrónica entraña riesgos de seguridad y fiabilidad. La maquinas de votación electrónica deberían poder ser auditadas hasta la última línea de código, para ello es necesario utilizar software libre o de código abierto y no software propietario, como ocurre en la actualidad. El principal problema es que el análisis de código es complejo y es imposible garantizar su fiabilidad al 100%. Por tanto la utilización del software libre es condición necesaria pero no suficiente.

> *En la "FAQ about the GNU GPL" aparece: "Fíjense, sin embargo, en que votar es un caso muy especial. Sólo porque el software dentro de un ordenador sea libre no significa que se pueda confiar en el ordenador para votar. Nosotros creemos que no se puede confiar en los ordenadores para votar. Votar debería hacerse en papel."*

2) La votación a través de redes telemáticas aporta mas complejidad al sistema electoral y por lo tanto mas riesgos, además de crear desigualdades sociales. Pero es necesario desarrollar este tipo de tecnologías por que son necesarias si queremos avanzar en el modelo de participación ciudadana a través de Internet.

3) El sistema de voto perfecto no existe, pero si se quiere implementar un sistema de voto electrónico, debe de existir una colaboración entre la Administración, los fabricantes, los expertos en informática, en derecho e incluso los propios ciudadanos, para entre todos delimitar los riesgos contra los que sería necesario protegernos, y crear unos estándares que permitan certificar los sistemas de voto electrónico.

Joaquín Domínguez Fernández

jdominguez@cortesaragon.es