

# Voto electrónico

## ¿Quién tiene realmente la decisión?

Gunnar Wolf — [gwolf@gwolf.org](mailto:gwolf@gwolf.org)

<http://gwolf.org/content/voto-electronico>

Instituto de Investigaciones Económicas UNAM  
Desarrollador del Proyecto Debian

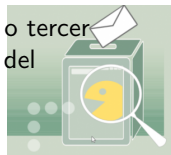
FISOL 2011 — Tapachula, Chiapas



# Mapa de ruta

A lo largo de esta presentación intentaré:

- 1 Explicar el concepto de *voto electrónico*: A qué se refiere, y –muy importante– a qué no
- 2 Presentar los principales puntos que motivan a muchos a creer que el voto electrónico es factible y deseable
  - Y demostrar que son falacias
- 3 Ilustrar, mediante ejemplos observados en diversos países a lo largo de las últimas décadas, las diferentes maneras en que las urnas electrónicas y diversos equipos relacionados pueden –y acostumbran– fallar
  - Esto, independientemente del país, de si es de primer o tercer mundo, de si la implementación es pública o privada, del tamaño de la empresa implementadora. . .



# Definiendo...

## ¿Qué sí es?

Reformas legales y argumentos técnicos orientados a instrumentar un proceso electoral donde la población (los votantes) empleen *urnas electrónicas*.

## ¿Y qué no?

Empleo de elementos informáticos como asistentes para la aritmética, el acopio, acumulación y difusión de los *resultados electorales*



## Definiendo...

### ¿Qué sí es?

Reformas legales y argumentos técnicos orientados a instrumentar un proceso electoral donde la población (los votantes) empleen *urnas electrónicas*.

### ¿Y qué no?

Empleo de elementos informáticos como asistentes para la aritmética, el acopio, acumulación y difusión de los *resultados electorales*



# Contenidos

- 1 Puntos a favor del voto electrónico
- 2 Disminución de costos
- 3 Agilidad en la obtención de resultados
- 4 Confiabilidad de los actores
- 5 Experiencias internacionales
- 6 Conclusiones



# ¡Magia electoral!



## Aparente punto a favor: Disminución de costos

- Un proceso democrático tradicional es caro.
- *Candados* para asegurar unicidad y legitimidad en cada boleta
- Mecanismos para asegurar que sólo los electores autorizados emitan su voto
- Garantías de no manipulación de todos los componentes antes, durante y después de la jornada electoral
- Necesidad de resguardar bodegas con el (inutil) material electoral por largos periodos de tiempo

La automatización del proceso ayudaría a implementar estos candados a un menor costo



## Aparente punto a favor: Agilidad en la obtención de resultados

- La demora en la publicación de resultados genera falta de confianza y suspicacia
- El tiempo que demora el conteo puede ser utilizado para instrumentar un fraude
- A través del voto electrónico, los resultados *oficiales* pueden ser anunciados prácticamente de inmediato al cerrar la última casilla



## Aparente punto a favor: Confiabilidad de los actores

- Muchos países han sufrido de diversos fraudes instrumentados con el sistema democrático *tradicional* a lo largo de la historia
- El elemento común a todos los fraudes es que son implementados por el factor humano
- Todos los actores involucrados son personas, por tanto, susceptibles a:
  - Compra de conciencias
  - Extorsión
  - Violencia física
  - No ser absolutamente neutros
- Si el proceso es controlado por computadoras, estos factores serían mitigados





# Contenidos

- 1 Puntos a favor del voto electrónico
- 2 Disminución de costos**
- 3 Agilidad en la obtención de resultados
- 4 Confiabilidad de los actores
- 5 Experiencias internacionales
- 6 Conclusiones



# El voto tradicional es caro

- Esto es un hecho incontrovertible
- Entre menos consolidada esté una democracia, más caro resulta cada voto
  - México es el país donde más caro resulta el voto en América Latina
  - Elecciones 2009 y 2010: Costos oficiales de 17 dólares (con algunas estimaciones de hasta 50 dólares incluyendo *gastos ocultos*) por voto
  - En una elección intermedia, con 40% de participación, de un total de 77 millones de votantes empadronados — hablamos de alrededor de 25 millones de votos
  - Por tanto, las elecciones de 2009 costaron **entre 523,600,000 y 1,540,000,000 dólares**
- «¿Y todo para qué...?»



# El voto tradicional es caro

- Esto es un hecho incontrovertible
- Entre menos consolidada esté una democracia, más caro resulta cada voto
  - México es el país donde más caro resulta el voto en América Latina
  - Elecciones 2009 y 2010: Costos oficiales de 17 dólares (con algunas estimaciones de hasta 50 dólares incluyendo *gastos ocultos*) por voto
  - En una elección intermedia, con 40% de participación, de un total de 77 millones de votantes empadronados — hablamos de alrededor de 25 millones de votos
  - Por tanto, las elecciones de 2009 costaron **entre 523,600,000 y 1,540,000,000 dólares**
- «*¿Y todo para qué... ?*»



## De candados y resguardos. . .

- Se ha argumentado que parte importante de esta verdadera fortuna proviene de la impresión y resguardo del material electoral antes, durante y después de la elección
- Sin embargo, estos costos palidecen si los ponemos junto al costo de compra (o renta) del equipo de votación. . .
- Y los contratos de mantenimiento. . .
- Y ni siquiera así podemos garantizar la seguridad de los resultados.
- Como veremos, ni siquiera resguardando físicamente a las mismas urnas.



## De candados y resguardos. . .

- Se ha argumentado que parte importante de esta verdadera fortuna proviene de la impresión y resguardo del material electoral antes, durante y después de la elección
- Sin embargo, estos costos palidecen si los ponemos junto al costo de compra (o renta) del equipo de votación. . .
- Y los contratos de mantenimiento. . .
- Y ni siquiera así podemos garantizar la seguridad de los resultados.
- Como veremos, ni siquiera resguardando físicamente a las mismas urnas.



## De candados y resguardos. . .

- Se ha argumentado que parte importante de esta verdadera fortuna proviene de la impresión y resguardo del material electoral antes, durante y después de la elección
- Sin embargo, estos costos palidecen si los ponemos junto al costo de compra (o renta) del equipo de votación. . .
- Y los contratos de mantenimiento. . .
- Y ni siquiera así podemos garantizar la seguridad de los resultados.
- Como veremos, ni siquiera resguardando físicamente a las mismas urnas.



## De candados y resguardos. . .

- Se ha argumentado que parte importante de esta verdadera fortuna proviene de la impresión y resguardo del material electoral antes, durante y después de la elección
- Sin embargo, estos costos palidecen si los ponemos junto al costo de compra (o renta) del equipo de votación. . .
- Y los contratos de mantenimiento. . .
- Y ni siquiera así podemos garantizar la seguridad de los resultados.
- Como veremos, ni siquiera resguardando físicamente a las mismas urnas.



## Costos absolutos: El equipo de votación

- El equipo de votación no es barato.
- Su adquisición, si mucho, puede justificarse prorrateándolo a lo largo de varias elecciones
- Pero los equipos deberán estar sometidos a vigilancia continua, incluso en los años que no será utilizado
- Debe recibir mantenimiento por parte de la empresa proveedora
- Debe haber equipos adicionales, distribuidos por todo el país, listos para reemplazar a una urna que presente un desperfecto



## Incluso siendo menos formal, el costo es demasiado alto

- El Tribunal Supremo de Elecciones de Costa Rica anunció (2009) que cancelaba el proceso de urnas electrónicas por su elevado costo
- El presidente del TSE, Luis Antonio Sobrado, hace también referencia a los riesgos que conllevaría la implementación completa del proyecto, incluyendo la conexión de urnas a red para la recopilación de datos (retomamos este punto en la siguiente sección)

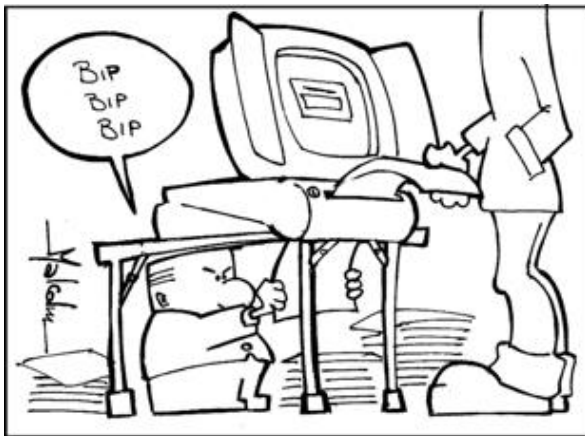


## No podemos confiar en las casualidades

- Ante un fallo del equipo (o del tendido eléctrico, o la necesidad de reubicar la casilla, o . . . ), la votación debe de todos modos llevarse a cabo
- En caso de fallo absoluto del equipo, la votación debe tener lugar utilizando como plan de respaldo papelería tradicional
- . . . ¿Y si el desperfecto ocurre tras media jornada de recepción de votos? ¿Se pierden los votos ya emitidos?
- El sabotaje selectivo se antoja como un excelente método para cancelar la voluntad de zonas con poblaciones *políticamente confundidas*



# Bip, bip, bib...



# Contenidos

- 1 Puntos a favor del voto electrónico
- 2 Disminución de costos
- 3 Agilidad en la obtención de resultados**
- 4 Confiabilidad de los actores
- 5 Experiencias internacionales
- 6 Conclusiones



# Un mundo acelerado

- Nos hemos ido obsesionando por la velocidad
- Los medios electrónicos nos han acostumbrado a que la información debe llegar a la sociedad de forma instantánea
- Al mismo tiempo, los sistemas electorales estipulan que –para no manipular una elección en proceso– no se deben dar a conocer los resultados parciales hasta que se cierre la última de las urnas
- Una vez que cierra la última urna, estamos acostumbrados a un periodo de demora de un par de horas para la presentación de los resultados *preliminares* y *no oficiales* (PREP)
- En una elección con un margen mayor al 5 %, es altamente probable que el PREP sea reflejo fiel de los resultados oficiales.



## ... ¡Y con justa razón!

Sociedad y medios se ponen muy nerviosos cuando la información  
no fluye pronto

A fin de cuentas, tenemos... Amplia experiencia

Entrevista en La Jornada con Manuel Bartlett, 2008

La decisión de no dar a conocer datos preliminares fue tomada por el presidente Miguel de la Madrid, dado que, cito: si se oficializaba en ese momento –con datos parciales– que Cárdenas Solórzano iba ganando, al final nadie aceptaría un resultado distinto.



## ... ¡Y con justa razón!

Sociedad y medios se ponen muy nerviosos cuando la información  
no fluye pronto

A fin de cuentas, tenemos... Amplia experiencia

### Entrevista en La Jornada con Manuel Bartlett, 2008

La decisión de no dar a conocer datos preliminares fue tomada por el presidente Miguel de la Madrid, dado que, cito: si se oficializaba en ese momento –con datos parciales– que Cárdenas Solórzano iba ganando, al final nadie aceptaría un resultado distinto.



## ... Algo hemos aprendido

- La experiencia del probable fraude de 1988 no se va a repetir (de forma exacta)
- El resultado de procesos electorales ahora se conoce alrededor de dos horas después de haber cerrado las últimas casillas
- ... Y sólo tarda más en casos de resultados muy cerrados — En cuyo caso se debe anunciar sin ambigüedad la causa de la demora (a diferencia del *se cayó el sistema*)



## ¿Cuánto mediría la ganancia?

Si empleáramos urnas electrónicas, ¿Cuánto tiempo ganaríamos?

- Ganaríamos sólo el tiempo empleado por los funcionarios de casilla en el escrutinio manual
- Es sólo una fracción del tiempo de verificación y protocolización
- Ganaríamos, frente al PREP. . . Un máximo de dos horas



## ¿Urnas electrónicas conectadas a red?

¿Podríamos reducir el tiempo de espera que implica la transmisión de resultados?

- Prácticamente ningún esquema de urna electrónica contempla la comunicación de resultados vía la red pública
- Prácticamente ningún país tiene cobertura de Internet en el 100 % de su territorio
- Y... No creo necesario siquiera mencionar la cantidad de vulnerabilidades que implicaría conectar una urna electrónica a Internet
- ¿Quién de ustedes resistiría el impulso de intentar vulnerarla?



## ¿Urnas electrónicas conectadas a red?

¿Podríamos reducir el tiempo de espera que implica la transmisión de resultados?

- Prácticamente ningún esquema de urna electrónica contempla la comunicación de resultados vía la red pública
- Prácticamente ningún país tiene cobertura de Internet en el 100 % de su territorio
- Y... No creo necesario siquiera mencionar la cantidad de vulnerabilidades que implicaría conectar una urna electrónica a Internet
- ¿Quién de ustedes resistiría el impulso de intentar vulnerarla?

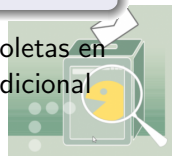


## Pero... ¿Puedo reducir tiempo y precisión de escrutinio?

Federico Heinz: «¿El voto electrónico mejora la democracia?»  
(2006)

Una alternativa factible es realizar la votación mediante formularios que contengan a todos los partidos, dejar que los votantes marquen su elección con tinta, y usar un scanner óptico para hacer un escrutinio automático, verificable mediante un simple recuento manual. No hay nada en contra de un escrutinio electrónico, pero digitalizar el acto mismo de la emisión del voto es extremadamente peligroso para la democracia.

Un scanner óptico permitiría la verificación de cientos de boletas en segundos, sin perder los atributos positivos del sistema tradicional



# ¡Espacio, que llevo prisa!



# Contenidos

- 1 Puntos a favor del voto electrónico
- 2 Disminución de costos
- 3 Agilidad en la obtención de resultados
- 4 Confianza de los actores**
- 5 Experiencias internacionales
- 6 Conclusiones



## ¿Qué nos preocupa cuidar en una elección?

- Diversos modos de fraude siempre han existido con el voto *tradicional* en papel
- Una de las promesas del voto electrónico es que reduce la posibilidad de modificar el total en la urna
- ... Hasta que consideramos *la manera* en que ésto podría realizarse — ¡Y resulta más preocupante aún!



# La naturaleza de un fraude tradicional

Se puede instrumentar un fraude de muy distintas maneras:

- Iniciando la jornada con una urna *embarazada*
- Introduciendo más de un voto a la urna
- Robando votos de la urna (o robando la urna entera)
- Introduciendo elementos que invaliden a otras boletas (p.ej. una bomba de tinta)
- Coaccionando a la población a votar en determinado sentido (o a no votar)



## Tipos de fraude que sólo la urna electrónica permite

- Con urnas electrónicas, algunos de los puntos anteriores quedan cubiertos — Pero se introducen otros mucho más poderosos
- Decirle al usuario una cosa, registrar otra
- Presentar resultados distintos al real
- Responder a umbrales de voto, modificando los resultados sólo en casos específicos
- Los errores lógicos... ¿Son fraude? ¿Son delito? ¿Qué son?



# Confianza en el software ya auditado

Incluso en el (improbable) supuesto de que se permitiera una auditoría completa, exhaustiva...

- ¿Cómo puedo asegurar que fue suficientemente profunda?
- ¿Cómo puedo asegurar que el código ejecutado es *verdaderamente* el código que fue auditado?
- Pocos especialistas pueden realizar bien esta tarea.  
¿Qué garantiza que puedo confiar en dichos especialistas?
- Universalidad de la capacidad de auditoría en el sistema tradicional
- Ejemplo: Sistema electoral eclesiástico (F. Heinz 2006)



# Confianza en el software ya auditado

Incluso en el (improbable) supuesto de que se permitiera una auditoría completa, exhaustiva...

- ¿Cómo puedo asegurar que fue suficientemente profunda?
- ¿Cómo puedo asegurar que el código ejecutado es *verdaderamente* el código que fue auditado?
- Pocos especialistas pueden realizar bien esta tarea.  
¿Qué garantía que puedo confiar en dichos especialistas?
- Universalidad de la capacidad de auditoría en el sistema tradicional
- Ejemplo: Sistema electoral eclesiástico (F. Heinz 2006)



## Las urnas electrónicas son *siempre* vulnerables

Feldman, Halderman y Felten publicaron un estudio a las estaciones de votación Diebold AccuVote-TS (las más difundidas para procesos electorales en EUA) en 2007

- Un usuario con conocimientos técnicos generales, aunque sin conocimiento específico de esta máquina, puede obtener acceso a reprogramar el equipo
- El ataque puede realizarse con un tiempo mínimo de acceso (comparable con el tiempo que un votante pasa a solas con el equipo)
- *Reprogramar* una urna electrónica no inserta uno, diez o cien votos en determinado sentido — Puede hacer cualquier modificación sobre los votos emitidos
- E incluso sobre los votos que *no han sido emitidos aún*



# Declaraciones del equipo de Feldman, Halderman y Felten

El equipo publica en su sitio Web un video de *diez minutos* demostrándolo: <http://citp.princeton.edu/voting/>

## Preguntas frecuentes en el sitio del equipo

- *Por qué estudiaron éstas máquinas Diebold? ¿Por qué no otras tecnologías para votos?*

Estudiamos estas máquinas porque son las que conseguimos. Si hubiésemos tenido acceso a otro tipo de máquinas, probablemente las hubiéramos estudiado.

- *¿Son otras máquinas más seguras que las que estudiaron?*

No lo sabemos. Esperamos que así lo sean —las elecciones dependen ya de ellas— pero no hay suficiente evidencia para responder a esta pregunta.

## Un *rastro impreso verificado* como única garantía

- Feldman, Halderman y Felten: *Un rastro impreso verificado por cada votante es la protección más importante que puede hacer más seguras a las máquinas de voto electrónico.*
- La única garantía que puede tener un votante de que su voto fue registrado correctamente es la generación de una boleta impresa de carácter irrevocable.
- Volveremos a este punto en la sección relativa a *la confianza en los actores*



# La imposibilidad de confiar en un sistema, cualquier sistema

Pero el problema es mucho más profundo que sólo vigilar *cajas*

- Citando a Ken Thompson (1984, «Reflections on trusting trust»), confiar en el estado interno de una computadora es sencillamente imposible
- Para confiar en un sistema de votación, es indispensable auditar el código del sistema
  - ... Y el código del framework en que fue escrito
  - ... Y de todas las bibliotecas con que está ligado
  - ... Y el código del compilador



# La imposibilidad de confiar en un sistema, cualquier sistema

Pero el problema es mucho más profundo que sólo vigilar *cajas*

- Citando a Ken Thompson (1984, «Reflections on trusting trust»), confiar en el estado interno de una computadora es sencillamente imposible
- Para confiar en un sistema de votación, es indispensable auditar el código del sistema
- ... Y el código del framework en que fue escrito
- ... Y de todas las bibliotecas con que está ligado
- ... Y el código del compilador



# La imposibilidad de confiar en un sistema, cualquier sistema

Pero el problema es mucho más profundo que sólo vigilar *cajas*

- Citando a Ken Thompson (1984, «Reflections on trusting trust»), confiar en el estado interno de una computadora es sencillamente imposible
- Para confiar en un sistema de votación, es indispensable auditar el código del sistema
- ... Y el código del framework en que fue escrito
- ... Y de todas las bibliotecas con que está ligado
- ... Y el código del compilador



# La imposibilidad de confiar en un sistema, cualquier sistema

Pero el problema es mucho más profundo que sólo vigilar *cajas*

- Citando a Ken Thompson (1984, «Reflections on trusting trust»), confiar en el estado interno de una computadora es sencillamente imposible
- Para confiar en un sistema de votación, es indispensable auditar el código del sistema
- ... Y el código del framework en que fue escrito
- ... Y de todas las bibliotecas con que está ligado
- ... Y el código del compilador



# La imposibilidad de confiar en un sistema, cualquier sistema

- ... Y el compilador utilizado para compilarlo
- ... y el compilador utilizado para compilar a ese compilador
- ... y el firmware de todos los dispositivos de la urna
- ... y llevar a cabo una verificación formal de la lógica del procesador y su chipset

Conseguir expertos capaces de llevar a cabo las verificaciones necesarias se vuelve imposible



# La imposibilidad de confiar en un sistema, cualquier sistema

- ... Y el compilador utilizado para compilarlo
- ... y el compilador utilizado para compilar a ese compilador
- ... y el firmware de todos los dispositivos de la urna
- ... y llevar a cabo una verificación formal de la lógica del procesador y su chipset

Conseguir expertos capaces de llevar a cabo las verificaciones necesarias se vuelve imposible



# La imposibilidad de confiar en un sistema, cualquier sistema

- ... Y el compilador utilizado para compilarlo
- ... y el compilador utilizado para compilar a ese compilador
- ... y el firmware de todos los dispositivos de la urna
- ... y llevar a cabo una verificación formal de la lógica del procesador y su chipset

Conseguir expertos capaces de llevar a cabo las verificaciones necesarias se vuelve imposible



# La imposibilidad de confiar en un sistema, cualquier sistema

- ... Y el compilador utilizado para compilarlo
- ... y el compilador utilizado para compilar a ese compilador
- ... y el firmware de todos los dispositivos de la urna
- ... y llevar a cabo una verificación formal de la lógica del procesador y su chipset

Conseguir expertos capaces de llevar a cabo las verificaciones necesarias se vuelve imposible



# El rol de control de la población en general

## Veredicto de la Suprema Corte de Alemania, 2009

Un procedimiento electoral en el que el elector no puede verificar de manera confiable si su voto fue registrado sin falsificación e incluido en el cálculo del resultado de la elección, así como comprender cabalmente de qué manera los votos totales emitidos son asignados y contados, excluye del control público a componentes centrales de la elección, y por lo tanto no alcanza a satisfacer las exigencias constitucionales.



## El caso brasileño

- Brasil usa urnas electorales desarrolladas localmente, empleando software libre
- En noviembre de 2009, el Tribunal Superior Electoral convocó a la comunidad de seguridad a encontrar vulnerabilidades
- Sergio Freitas da Silva logró –monitoreando radiaciones electromagnéticas con equipo casero– leer a distancia por quién emitía su voto cada votante
- ... Rompiendo el principio de secreto electoral



## ¿Qué constituye una *demostración formal*?

En el caso de Brasil. . .

- Si bien en los términos de la convocatoria ningún equipo pudo modificar la información, nada indica que esto sea imposible
- De hecho, estudios posteriores sí llevaron a modificación de datos registrados en las urnas
- Hay que mantener en mente que la *ausencia de evidencia no es evidencia de ausencia*.
- Puede haber muchas fallas no detectadas — Especialmente, puede haber *puertas traseras* intencionales escondidas.



# La fiabilidad de la modernidad



# Contenidos

- 1 Puntos a favor del voto electrónico
- 2 Disminución de costos
- 3 Agilidad en la obtención de resultados
- 4 Confiabilidad de los actores
- 5 Experiencias internacionales**
- 6 Conclusiones



# Algunos ejemplos de fallos monumentales

- Esta lista va sólo para ejemplificar algunas vivencias en diversos países del mundo
- No busca ser comprensiva, sólo ilustrativa
- Hay muchos casos de experiencias exitosas también
  - Pero no lo olviden: *La ausencia de evidencia no es evidencia de ausencia.*



## California, EUA, 2004

- La empresa Diebold sometió a certificación un modelo y versión específico de sus urnas electrónicas, y fue aprobado
- Sin embargo, para la elección en cuatro condados (municipios), se utilizó otro
- Kevin Shelley, Secretario de Estado de California, prohibió el uso de dichos equipos, y retiró la certificación
- ¿Qué habrá querido esconder la empresa en esa versión que no era? El cambio no fue gratuito/accidental.



## California, EUA, 2004

- La empresa Diebold sometió a certificación un modelo y versión específico de sus urnas electrónicas, y fue aprobado
- Sin embargo, para la elección en cuatro condados (municipios), se utilizó otro
- Kevin Shelley, Secretario de Estado de California, prohibió el uso de dichos equipos, y retiró la certificación
- ¿Qué habrá querido esconder la empresa en esa versión que no era? El cambio no fue gratuito/accidental.



## Montreal, Canadá, 2005

- La elección municipal fue realizada con urnas electrónicas
- 45,000 votos fueron contabilizados doblemente
- La autoridad electoral publicó un reporte, indicando la necesidad de tener acceso completo al código fuente, pruebas de funcionalidad, plan de respaldo, y medidas estrictas para el almacenamiento y resguardo

### Marcel Blanchet, Funcionario Electoral en Jefe

(...) Son tecnologías vulnerables. La manera en que fueron manejadas no ofrece suficiente garantía de transparencia y seguridad para asegurar la integridad del voto.

## El mini-bar de Felten

- Ed Felten consiguió una urna electrónica de Diebold (la misma empresa que fabrica casi todos los cajeros automáticos bancarios del mundo), en 2006
- Estas urnas vienen protegidas de intervención por parte de los usuarios con una llave
- ... Felten encontró que las urnas pueden ser abiertas por las llaves genéricas maestras de cajones de oficina y minibares de hotel
- Abriendo la urna, se puede reemplazar incluso el programa que registra los votos



## Nueva Jersey 2008: Error aritmético

- Felten reveló también el reporte de una estación de voto en el estado de Nueva Jersey
- Si hay algo que una computadora debería saber hacer bien...  
Es sumar
- Sin embargo, el papel impreso presentando los resultados presentaba un error aritmético: Los votos emitidos por cada opción no concordaban con los votos totales



## Las Grutas, Argentina, 2007

- En Las Grutas, provincia de Río Negro, se utilizaron urnas electrónicas en 2007
- El padrón electoral tenía amplias discrepancias con el digital: En las mesas tradicionales la participación fue del 70 %, pero en las digitales alcanzó apenas el 40 %
- Al intentar extraer los resultados las autoridades de casilla, por error, una de las urnas eliminó los registros en vez de transferirlos a una memoria externa
- El ciudadano Sergio Daniel Plos presentó un amparo para que la localidad no volviera a participar en elecciones electrónicas — El 10 % de los votantes se adhirió al reclamo



## Virginia y Pensilvania, 2008

En las elecciones federales de EUA en 2008, varias urnas en Virginia y Pensilvania registraron descomposturas. Dependiendo de la jurisdicción local:

- Algunas mesas no se abrieron, con lo cual amplios grupos no pudieron ejercer su derecho a voto
- Otras mesas se abrieron con votación tradicional, pero sin papeleía electoral (sino con hojas estándar de papel), con lo cual no había garantías adecuadas de unicidad en el voto



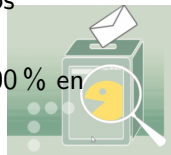
## Partido Laborista, Israel, 2008

- Las urnas empleadas para las elecciones internas del Partido Laborista tenían problemas de usabilidad/sensibilidad
- Algunos votantes reportaban que el sistema no era suficientemente sensible y no les permitía votar
- Otros reportaban que el sistema registró un voto antes de haber sido tocado, o marcando una opción distinta a la seleccionada
- El partido tuvo que cancelar la votación, y repetirla al día siguiente con papeletas tradicionales



## Holanda, 2007

- Holanda es uno de los primeros países en desplegar ampliamente estaciones de voto electrónico
- En 2007, el grupo *Wij vertrouwen stemcomputers niet* (*No confiamos en las computadoras votantes*) presentó en vivo, en televisión nacional, la demostración de cómo podían reprogramar una urna
- La Comisión Asesora en Procesos Electorales revirtió en 2008 la recomendación que llevó a la implementación del voto electrónico, y rechazó la propuesta de introducir una nueva generación que corregía el fallo por el cual entraron los atacantes
- Hoy en día, los procesos electorales holandeses son 100% en papel, con conteo manual



# EVM: La India, 2010

- La India es la democracia representativa más grande del mundo, uno de los países más complejos, y desde hace dos décadas, casi la totalidad de sus procesos están basados en la urna electrónica *EVM*
- El funcionamiento del EVM se había manejado como un secreto, hasta que en abril de 2010, Alex Halderman, Hari Prasad y Rop Gonggrijp consiguieron un equipo
- Publicaron dos ataques que pueden llevarse a cabo en unos cuantos minutos (el tiempo justo para realizarlos dentro de una casilla de votación) que permiten alterar los resultados



# El valor del voto



# Contenidos

- 1 Puntos a favor del voto electrónico
- 2 Disminución de costos
- 3 Agilidad en la obtención de resultados
- 4 Confiabilidad de los actores
- 5 Experiencias internacionales
- 6 Conclusiones**



# Conclusiones

- No podemos ser ajenos a la importancia de rechazar los intentos por imponernos votos electrónicos
- Como ciudadanos, debemos estar atentos a las iniciativas y participar, impugnar cuando avancen estas propuestas
- Como profesionales del cómputo, debemos negarnos a participar –incluso cuando esto nos presente una oportunidad de negocios– en la implementación de este tipo de tecnología
- Es común que nuestra sociedad, poco politizada y muy escéptica, busque no inmiscuirse en temas áridos y espinosos como la política
- Pero si buscamos que nuestra sociedad cambie, ¡debemos comenzar por involucrarnos!



# La importancia que damos al fenómeno



# ¿Dudas?

¡Gracias!

Gunnar Wolf — [gwolf@gwolf.org](mailto:gwolf@gwolf.org)

<http://gwolf.org/content/voto-electronico>

