OBSERVATORIO VOTO ELECTRÓNICO, **INFORME 2M6**

Así, no

2M6: Informe tecnológico del Observatorio Voto Electrónico (OVE) sobre la PVI, Prueba de Voto por Internet, realizada en el Reino de España con motivo del Referéndum sobre el *Tratado por el que se establece una Constitución para Europa,* que compromete a 2 millones de electores y el 6% del censo, sin valor vinculante.
Entidades organizadoras: Junta Electoral Central (resolución 25/01/05), Ministerio del Interior e Indra Sistemas, S.A.
Emisión: 21 de Febrero a las 00,01 horas
Anotación. El OVE es firme partidario del despliegue de infraestructuras de voto electrónico presencial y remoto (por Internet) y a tal tarea ha dedicado y dedica sus esfuerzos. Somos partidarios, asimismo, que dicho despliegue se efectúe sin poner en peligro, gratuita, las garantías jurídicas de cualquier proceso electoral. El despliegue de este tipo de infraestructuras es inaplazable, pero en ningún modo son fáciles o se pueden improvisar. Más información sobre el OVE y su actividad en http://www.votobit.org

OBSERVATORIO
VOTO ELECTRÓNICO

Conclusión General

El OVE ha podido demostrar que la PVI (Prueba de Voto por Internet), realizada en el Reino de España, y cuya seguridad y fiabilidad descansaba en la negación del valor del escrutinio público —opacidad del proceso—, ha sido una ilusión óptica. Las premisas y objetivos del voto electrónico son tres:

1. Facilitar el recuento
2. Proporcionar al procedimiento mayores garantías que las actuales (fiabilidad y confiabilidad)
3. Proporcionar al votante mayor seguridad que la del sistema actual (no coerción, no repudio, universalidad).

De estas premisas, sólo se cumple la primera. El OVE demuestra con el presente informe que la aplicación que soporta la PVI no es apta para el fin que se propone. Se han detectado niveles intolerables de vulnerabilidad**.**

Errores dramáticos

1. La PVI, —por sus características, por el volumen de población que ha pretendido abarcar—, se ha efectuado **no cumpliendo**, repetimos, **no cumpliendo** requisitos elementales de información pública y transparencia, que se han saldado con una bajísima participación.
2. La PVI es relevante para la formación de antecedentes por **a) no cumplir**, repetimos, **no cumplir**, el requisito básico que exigía la Junta Electoral Central de confidencialidad del voto (puntos 5, 6, 9,10 y 12 de Elementos Probatorios) en su resolución del 25/01/05 y **b)** por carecer de una autoridad reconocible e identificable para emitir una opinión cualificada del resultado de la experiencia. El OVE elevará una petición razonada a la Junta Electoral Central para que resuelva dejar sin valor, a todos los efectos, la PVI.
3. La PVI se ha realizado dentro de un proceso autocontenido: quienes realizan y ejecutan las pruebas se autovalidan, en este caso el Ministerio del Interior como gestor de la administración electoral y el operador privado implicado Indra Sistemas, S.A., con indefensión de la Junta Electoral Central, sin espacio para la opinión cualificada y experta e ignorando que estamos ante tecnologías altamente sensibles por el "daño país" inmenso y gratuito que puede ocasionar el despliegue de soluciones inadecuadas.

4. El seguimiento realizado por el OVE aporta elementos de juicio probatorios sobre la inadecuación de los recursos de ingeniería empleados en la PVI que nos ocupa.
5. La PVI ha constituido un acontecimiento desgraciado, explicable por la indefensión de la Junta Electoral Central, sin opinión experta de respaldo, comprometiendo la honorabilidad y espíritu de cooperación de los ayuntamientos implicados. Corporaciones que en ningún momento han pretendido abusar de la confianza de sus vecinos. Al revés, han pretendido, en todo momento, como se desprende de sus pronunciamientos públicos, ser un canal activo de colaboración para el fomento de las nuevas infraestructuras.
6. El OVE deduce, a la luz de los hechos, que las partes implicadas, Ministerio del Interior e Indra Sistemas, S.A. no reúnen capacidades para monitorizar y administrar una hipotética administración electoral electrónica a tenor de la acumulación de despropósitos que coinciden en la PVI.
7. En opinión del OVE la Junta Electoral Central es la única autoridad competente y a ella, y sólo a ella, le debe corresponder la administración directa sin administraciones interpuestas de los procesos electorales.
8. La Junta Electoral Central necesita el concurso de asesores o consultores cualificados, para acometer el salto hacia nuevas infraestructuras de voto. Conviene no olvidar que las infraestructuras que nos ocupan, su funcionalidad, son de naturaleza expansiva y altamente crítica.
9. El despliegue de las nuevas infraestructuras de voto electrónico debe hacerse con transparencia, periodos de información adecuados y apertura de los recursos tecnológicos a utilizar a la auditoría externa y al escrutinio público. No existen más opciones o vías mediadas. Todo lo que no sea transparencia es ofuscación y maniobras para ocultar intereses maliciosos.
10. El procedimiento seguido para la adjudicación a Indra Sistemas, de la PVI, no es un procedimiento correcto. Indra Sistemas se ha convertido en la empresa operadora de la PVI mediante su oferta de mejora en un concurso para la renovación del SIRE (Sistema Integrado de Recuento Electoral), en la que ofrecía su tecnología para ejecutar una prueba de voto masivo por Internet.
11. En adelante, y con el único afán de generar una infraestructura robusta y redundante, nuestra mejor opinión es descomponer el concurso por áreas geográficas para todas aquellas empresas que cumplan los estándares que señale la Junta Electoral Central, mediante tecnologías adecuadas dentro de un entorno altamente protegido. Concurso que debiera estar reglado y supervisado por la Junta Electoral Central.
12. Sería deseable que la aplicación desarrollada por Indra Sistemas, S.A. para la PVI y la(s) máquina(s) que compromete, se inmovilizaran por mandato de la Junta Electoral Central y se permitiera a un grupo de expertos, entre los que debería estar el OVE, su auditoría completa para ampliar información.

Elementos Probatorios

1. No existen protocolos de actuación, de despliegue, de arranque, de operación, de escrutinio y de parada de la solución de voto electrónico. **No existen, o si existen no se han hecho públicos.** Bajo ningún concepto, pueden ser ofuscados u ocultados al escrutinio público.
2. No existe documentación de referencia que pueda ser consultada sobre la arquitectura de hardware y software o en su defecto las auditorías que son prescriptivas, las piezas de código (abiertas) y los algoritmos que se están utilizando. Lo que hace robusto un sistema de voto electrónico es la transparencia. Son las claves de cifrado lo que le hacen invulnerable, al lado de servidores en entornos protegidos, junto adecuados protocolos de operación y un cliente, en la máquina del elector, resistente al espionaje y los ataques maliciosos.
3. La aplicación de voto electrónico que se instala en el ordenador de los electores no es universal, corre, exclusivamente, en sistemas operativos de la empresa Microsoft, específicamente Windows XP, 2000 y NT. Los millones de usuarios de Windows 98 tampoco pueden votar.
4. El certificado raíz está ofuscado en un trozo de código javascript, sin nada que lo justifique. El votante no puede comprobar su validez, sólo su integridad.
5. Puesto que una parte de la clave del elector es el DNI, el procedimiento por el que se separan la identidad del votante y el valor de su voto no está demostrado. El OVE desistió por falta de tiempo del chequeo de la ingeniería de software y se reserva su propia opinión.
6. No existe seguridad en la confidencialidad del voto, ya que el emisor tiene en su poder

TODAS las firmas digitales utilizadas en el procedimiento, tanto públicas, como **privadas**.

7. El elector no recibe testimonio de que ha votado, de que su voto ha sido trasladado a las autoridades competentes para su escrutinio y que efectivamente su voto ha sido computado y no manipulado.
8. La aplicación destinada al cliente puede ser **inutilizada** fácilmente, **impidiendo** su instalación en la máquina del elector e **impidiendo** el ejercicio del derecho al voto.
9. La aplicación diseñada para ser instalada en la máquina del elector permite **conocer**, mediante un código malicioso, el valor del voto.
10. La aplicación diseñada para ser instalada en la máquina del elector permite **modificar** el valor del voto mediante código malicioso.
11. Puesto que el nivel de formación del votante ha sido muy deficiente, el applet de Java oficial podría ser sustituido por otro, malicioso, con un muy alto nivel de éxito.
12. La protección del servidor de respaldo para toda la PVI, que se identifica como servidor del Ministerio del Interior, padecía vulnerabilidades gravísimas y da buena prueba de ello el paso franco desde el exterior al menú de votaciones. Haciéndose vulnerable para cualquier persona, grupo, banda, entidad o país con objetivos maliciosos.
13. La aplicación que respalda la PVI es extremadamente sensible a entornos hostiles. Un ordenador casero se considera un entorno hostil. Es conocido el abandono por parte del gobierno USA de un proyecto más sofisticado que el presente por esta vulnerabilidad (proyecto SERVE). Puede consultarse al respecto el conocido informe negativo de Avi Rubin, notoria autoridad mundial en seguridad. http://servesecurityreport.org/
14. La gestión de los certificados de la aplicación que respalda la PVI, no sigue los estándares.
15. La navegación que se muestra al votante no sigue los estándares sobre accesibilidad y usabilidad comúnmente admitidos.

ANTECEDENTES

El OVE solicitó, repetidas veces, por varios conductos, ser acreditado para realizar una observación tecnológica de la PVI, Prueba de Voto por Internet, considerando la envergadura del campo sociológico, 2 millones de potenciales electores y la imperiosa necesidad de escrutinio público y auditoría externa que estos procesos requieren. No hemos obtenido respuesta en ningún caso, viéndose obligado el OVE, cuya trayectoria pública es bien conocida, a realizar el escrutinio de la solución tecnológica, para prestar un servicio al interés general.

La fuerte, y legítima, presión empresarial que estos procesos promueven, aún más si se considera la cuantía económica de los contratos que están en juego, ha demostrado en procesos parecidos: **a)** que el desbordamiento legal tiende a comprometer los derechos políticos de los ciudadanos; **b)** la pasmosa fragilidad de las autoridades electorales, exentas de estructuras de consulta y asesoramiento experto, para juzgar y valorar los nuevos acontecimientos tecnológicos; **c)** la inadecuación de la administración electoral delegada, el Ministerio del Interior, para tomar decisiones sobre tecnologías críticas que desconocen; y **d)** que empresas no aptas, o poco cualificadas, abusen de su posición para adjudicarse los contratos que están en juego sin mérito para ello y poniendo en peligro la credibilidad de una nación.

En el caso que nos ocupa se ha dado, a su vez, un pésimo funcionamiento entre la Autoridad Electoral, la Junta Electoral Central, la Administración Electoral Delegada, el Ministerio del Interior, y la empresa operadora de la solución tecnológica, con funciones solapadas y la indefensión de los ciudadanos y electores.

El OVE, en todo caso, remitió por correo certificado al Ministerio del Interior y a la Junta Electoral Central un abanico de preguntas que nos parecían sustantivas, de interés general, para el correcto desenvolvimiento de la presente prueba piloto. No han sido contestadas. El formulario es consultable en http://www.votobit.org. Con los antecedentes descritos, el OVE, a ciegas, con un nivel de información cero, se dispuso a la evaluación de la aplicación que promueven el Sr. Ministro del Interior y la empresa Indra Sistemas, S.A. como altamente segura y eficiente. Se ha evaluado en un tiempo récord, con las limitaciones que tal circunstancia impone, para determinar si la aplicación de voto electrónico, respondía a las recomendaciones del Consejo de Europa

—Rec(2004)11 of the Committee of Ministers—, a las que el propio OVE considera imperativas, y si la PVI podía dañar o amenazar los derechos políticos de los españoles.

Los resultados obtenidos de nuestra auditoría, realizada en condiciones muy adversas, pero de la que han podido extraerse argumentos concluyentes, nos obligan a considerar la PVI en su conjunto, desde su organización, su despliegue y la propia aplicación, sin paliativos, un rotundo fracaso.

Errores de concepto y diseño en la aplicación que respalda la PVI

1. La ausencia de separación de poderes (autenticación, votación y custodia). No sólo eso, sino que el servidor web forma parte intrínseca del sistema de votación, compartiendo incluso certificados.
2. La centralización de servicios en un único servidor. NO existe una aplicación distribuida por colegios o distritos electorales. El ataque por denegación de servicio es obviamente un problema.
3. La implementación concede demasiada "inteligencia" al equipo cliente, que por definición debería ser considerado "hostil" y no confiable. Esto redunda en posibilidades de bloqueo y fraudes, debido a incorrectas configuraciones, o bien por ataques "man on the middle" (suplantación de personalidad).
4. La ausencia de garantías para el votante: **a)** no hay emisión de acreditación de voto; **b)** no hay procedimientos de revocación; **c)** no hay procedimiento de impugnación ni de verificación; **d)** ni siquiera hay procedimientos para garantizar que el votante es el único poseedor de su certificado.
5. Es posible descargar, descompilar y analizar tanto las páginas como los applets, javascripts, y bibliotecas dinámicas.
6. Los errores de ingeniería de software permiten acceder al menú de votaciones.

Pruebas realizadas

1. Estudio del entorno: sistema operativo, servidor, aplicaciones requeridas, consideraciones de seguridad, accesibilidad, portabilidad
2. Descarga de los diversos scripts, applets, bibliotecas dinámicas y páginas web de manera externa a la aplicación.
3. Análisis de la aplicación. Diagramas de flujo, dependencias. Estructuras de datos, ofuscación de código y resistencia a la ingeniería inversa. Búsqueda de deficiencias en la codificación. Resistencia a la inyección de código.
4. Análisis del manejo de certificados: descarga, importación/exportación. Análisis del árbol de autoridades, uso de certificados externos, suplantación de CA y de certificados, manejo de CRL's. Procedimientos de cifrado y firma, análisis de la conexión segura con el servidor
5. Ataques al sistema: Inyección de código, substitución de DLL's, modificación de la seguridad en el cliente, ataques a la seguridad de los applets, uso de otras máquinas virtuales java. Estudio de la estabilidad. Resistencia al ataque por denegación de servicio. Estudio del hardware implicado. Posibles influencias de virus, spyware y troyanos. Entrada simultanea desde varios equipos con el mismo usuario.
6. Emisión del voto. Control de si el usuario ha votado ya o no. Gestión de recursos locales en cliente (cookies y registro).
7. Ataques al servidor. Acceso al sistema. Bloqueos de comunicación cliente-servidor, falsificación de certificados. Inyección de CA's falsas.

Estudio del sistemas de manejo de certificados

En la obtención y análisis del certificado, el sistema falló:

1. La aplicación, en lugar de seguir los procedimientos estándar para emisión y descarga de certificados, válidos para todos los navegadores y sistemas, intenta descargar unas bibliotecas DLLs (bibliotecas de enlace dinámico), específicas para Windows.
2. El sistema, algo insólito, intenta enviar al servidor la clave privada, acción prohibida según todos los estándares de seguridad conocidos. Es una acción que permite a la aplicación conocer la identidad digital del votante y suplantarle si ese fuera su propósito. Los procedimientos de

autentificación, confianza y no repudio quedan invalidados.
3. Cualquier ataque exitoso al servidor está en condiciones de robar los certificados de todos los usuarios.
4. El procedimiento no es compatible con la autentificación mediante claves generadas y almacenadas en tarjetas criptográficas. El futuro DNI basado en este tipo de tarjetas no podría funcionar.
5. No es posible descargar el certificado raíz de la autoridad de certificación. Las implicaciones son evidentes. No se puede comprobar su validez, solo su integridad. El certificado raíz, atención, viene ofuscado en un código javascript e incluye hasta CINCO certificados raíz. De ellos se deduce que algunos son de prueba, otros correspondientes a otras votaciones y entidades y uno de ellos no posee ningún tipo de identificación. Con diversos tipos de certificados se puede acceder a la aplicación. A más, el certificado raíz del servidor web y el de los certificados es el mismo. La autoridad de certificación es el MIR que a su vez está acreditado por Thawte (Premiun CA).
6. Es perfectamente posible desde una consola javascript, inyectar y ejecutar código en una página, inyectar nuevos certificados raíz que autentifiquen en el cliente certificados distintos a los originalmente esperados.
7. Dado que el único control y validación de los certificados se realizaría en el cliente, sería pues posible acceder al servidor con una identidad robada o falsa.

Manejo de la aplicación de voto

1. Diversos errores permiten descargar y examinar el applet de java (votación) de manera separada, y las bibliotecas de DLLs. Los scripts, applets, y dll's quedan a disposición de todo tipo de ataques. La instalación del entorno Java 'j2re-1.4.3' se realiza por cualquier usuario, así como los applets, drivers y bibliotecas dinámicas.
2. La aplicación EXIGE del cliente la anulación de todas las políticas de seguridad en cuanto al acceso al servidor. Cualquier ataque por suplantación de personalidad tendría éxito.
3. Se pueden anular las políticas de seguridad de la máquina virtual java del cliente y por lo tanto, los applets y sus contenidos.
4. El sistema se inutiliza completamente impidiendo el derecho al voto programando una infección viral sobre alguna de las bibliotecas descargadas.
5. No existen políticas de control de sesiones o de acceso y no se usa ningún mecanismo de autentificación del cliente en el establecimiento de la conexión SSL.
6. El servidor no está firmado por ninguna autoridad de Certificación establecida de serie en el navegador. Es preciso instalar dicha certificación.
7. Es posible acceder desde el exterior a la sesión de voto del elector, inyectando javascript, invocando los métodos contenidos en los applets y sustituyendo los API's.
8. Sin introducir ningún tipo de contraseña es posible acceder desde el arranque de la máquina hasta la emisión del voto. Cualquier usuario puede apropiarse de cualquier certificado sin contraseña alguna y presentarse ante el entorno de voto con cualquier acreditación que contenga el sistema.
9. No se respetan los estándares de accesibilidad y usabilidad con grave perjuicio para los discapacitados, particularmente los invidentes.

Funcionamiento de la aplicación

1. La aplicación genera procesos de validación redundantes sin interés desde el punto de vista de la seguridad. Se realizan en el entorno del cliente, son inoperantes y fácilmente abatibles. El procedimiento de cifrado y firma del voto no es oculto. Sería posible generar de manera externa votos válidos.
2. De los procedimientos de la PVI se deduce que el administrador de la aplicación disfruta de procedimientos de revocación del certificado. Plantea legítimas dudas sobre el secreto del voto, y el sistema de custodia y recuento.

Auditoria de seguridad

Servidor Web

El servidor www.evoto.mir.es se encuentra correctamente configurado y está situado en el parque de servidores de la Guardia Civil como anuncian sus mensajes de error y el dominio mir.es. Asimismo los firewalls de la red de la Guardia Civil están correctamente configurados.

Detalle de pantalla

La transmisión a nivel de red va encriptada con SSL desde que se establece la aceptación del certificado web SSL que está emitido por http://www.thawte.com. La información que pasa por el cable de red nunca viaja sin encriptar por internet.

El servidor Web de la máquina cert.mir.es y evoto.mir.es son servidores web 'Sun-one-Web-Server/6.1' y, aunque tiene parches, no se conoce ningún error público del mismo, por ahora. Los testeos no han dado ningún resultado negativo acerca de su seguridad. Se debería eliminar el 'header' (cabecera identificativa) del servidor web para no dar información acerca de la versión de servidor que alberga la página. Reduciría muy considerablemente las posibilidades de que si sale un bug fuera usado maliciosamente para modificar las votaciones.

Situaciones no testadas

Las pruebas realizadas han sido parciales. No están hechas con ánimo intrusivo, sino con ánimo de identificación y análisis de la arquitectura de hardware y software, con criterios de evaluación. Tienen un ritmo distinto a los ataques intrusivos que pretenden debilidades y destrozos. No se han podido realizar pruebas basadas en la estabilidad del servidor, tampoco en la configuración de la alta disponibilidad de los mismos, ni en la robustez del caudal que los abastece. Aunque el OVE ha podido formar sus opiniones, en la práctica, no se ha podido confirmar, fehacientemente, determinados supuestos, de importancia crítica para valorar la adecuación de las infraestructuras que tienen que soportar una votación real.

Es imprescindible saber si el firewall está optimizado para responder a ataques por saturación de caudal. No se conoce la opinión del operador de la PVI sobre la alta disponibilidad y su estrategia de despliegue. Se desconoce el criterio del operador de la PVI sobre los proxys inversos o granjas de servidores para soportar un número muy alto y simultáneo de conexiones a la aplicación en una situación real —según el Manual del Registrador entregado a los centros de votación este error aparece mencionado como común—. De igual modo, se desconoce la opinión que merecen al operador de la PVI las bases de datos instaladas en un sistema redundante de almacenamiento RAID, con alimentación eléctrica y controladores de disco redundantes y separados físicamente por localización geográfica. Y otros extremos de similar interés.

No universalidad de la aplicación que soporta la PVI

Queremos resaltar la siguiente porción de código javascript que se encuentra en la página inicial de acceso al sistema de voto.

```
<SCRIPT LANGUAGE=Javascript>
function envia(){

document.f.submit();
```

```
}

if (navigator.userAgent.indexOf('IRIX') != -1) {var SO = "Irix"; alert('La aplicación de
Voto no esta soportada para el sistema operativo IRIX'); }
else if ((navigator.userAgent.indexOf('Win') != -1) &&
(navigator.userAgent.indexOf('98') != -1)) {var SO= "Windows 98";alert('La aplicación de
Voto no esta soportada para el sistema operativo Windows 98 o Millenium');}
else if ((navigator.userAgent.indexOf('Win') != -1) &&
(navigator.userAgent.indexOf('95') != -1)) {var SO= "Windows 95";alert('La aplicación de
Voto no esta soportada para el sistema operativo Windows 95');}
else if (navigator.appVersion.indexOf("16") !=-1) {var SO= "Windows 3.1;alert('La
aplicación de Voto no esta soportada para el sistema operativo Windows 3.1');"}
//else if (navigator.userAgent.indexOf("NT 5.1") !=-1) {var SO= "Windows XP"}
//else if (navigator.appVersion.indexOf("NT") !=-1) {var SO= "Windows NT"}
else if (navigator.appVersion.indexOf("SunOS") !=-1) {var SO= "SunOS";alert('La
aplicación de Voto no esta soportada para el sistema operativo SunOS');}
else if (navigator.appVersion.indexOf("Linux") !=-1) {var SO= "Linux";alert('La
aplicación de Voto no esta soportada para el sistema operativo Linux');}
//else if (navigator.userAgent.indexOf('Mac') != -1) {var SO= "Macintosh"}
//else if (navigator.appName=="WebTV Internet Terminal") {var SO="WebTV"}
else if (navigator.appVersion.indexOf("HP") !=-1) {var SO="HP-UX";alert('La aplicación
de Voto no esta soportada para el sistema operativo HP-UX');}
else {var SO= "No identificado"}
</SCRIPT>
```

El código analiza los sistemas operativos que no están soportados, que son muchos: ni Linux, ni los UNIX más utilizados, ni siquiera muchos de los sistemas operativos de Microsoft.

Lo reseñable es que en los primeros días de la votación éste código no existía, lo que demuestra una fase muy breve o inexistente de pruebas y certificación de la aplicación. Situación extraña, dado que Indra ha de cumplir para sus proyectos las normas de calidad ISO, que obligan realizar este tipo de pruebas y elaborar un informe.

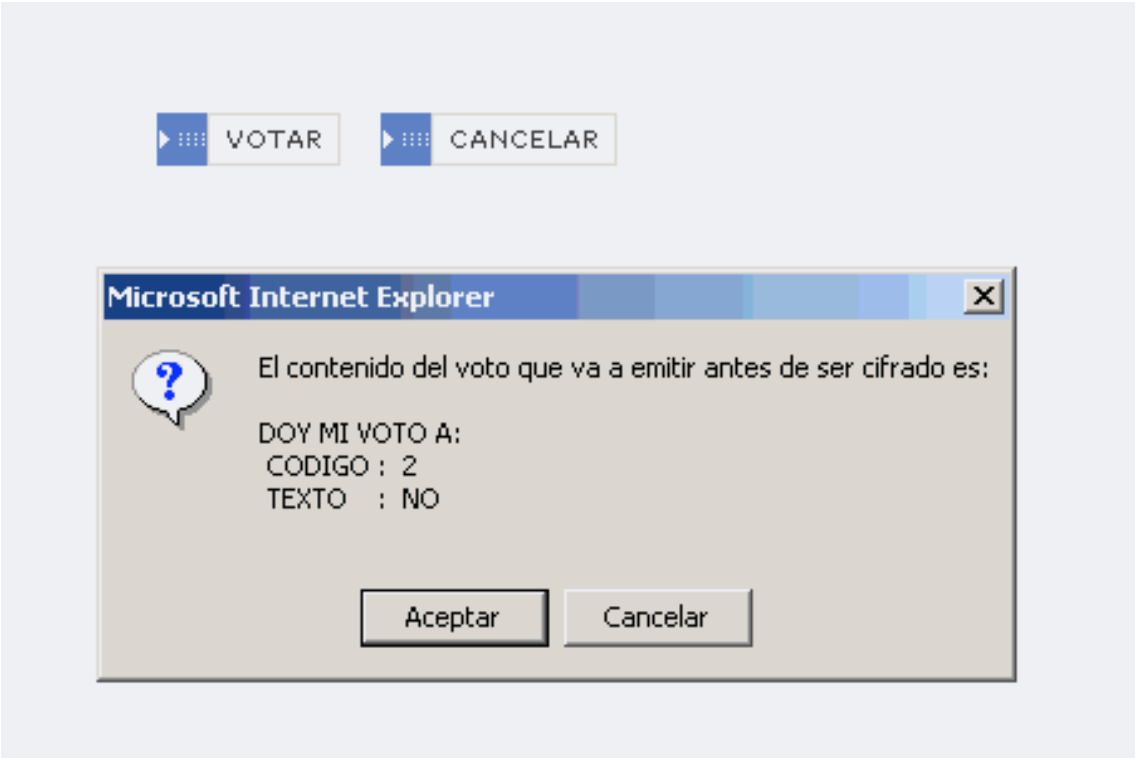
A pesar de las indicaciones del código la aplicación tampoco soporta el Macintosh, MacOSX, ni con Internet Explorer, Firefox, Safari, Opera o Mozilla.

Cancelación de la descarga del certificado

Si por error se cancela la descarga del certificado, no se volverá a producir la carga correcta del mismo. El responsable de esta operación es el javascript que se llama 'InicioApp.js'. Es un instante confuso para el votante y no se contemplan instrucciones en caso de no tener certificado instalado. El autor del código de la aplicación dice lo siguiente:

```
//Verifico que el applet esté cargado correctamente ya que si no se carga
        //ahora correctamente ya nunca lo hará y es necesario que esté cargado para
        //votar (Si no fuera por esto con usuario/contraseña no sería necesario
        //cargar el applet
        if (!( CompruebaCarga() == true ))
        {
                //Si el applet no está cargado correctamente (El mensaje ya lo ha
gestionado
                //la funcion CompruebaCarga) sale
                return false;
        }
```

Códigos maliciosos



Pantalla de aviso, nos da un mensaje mencionando 'Código 2' (Muy confuso para el votante)

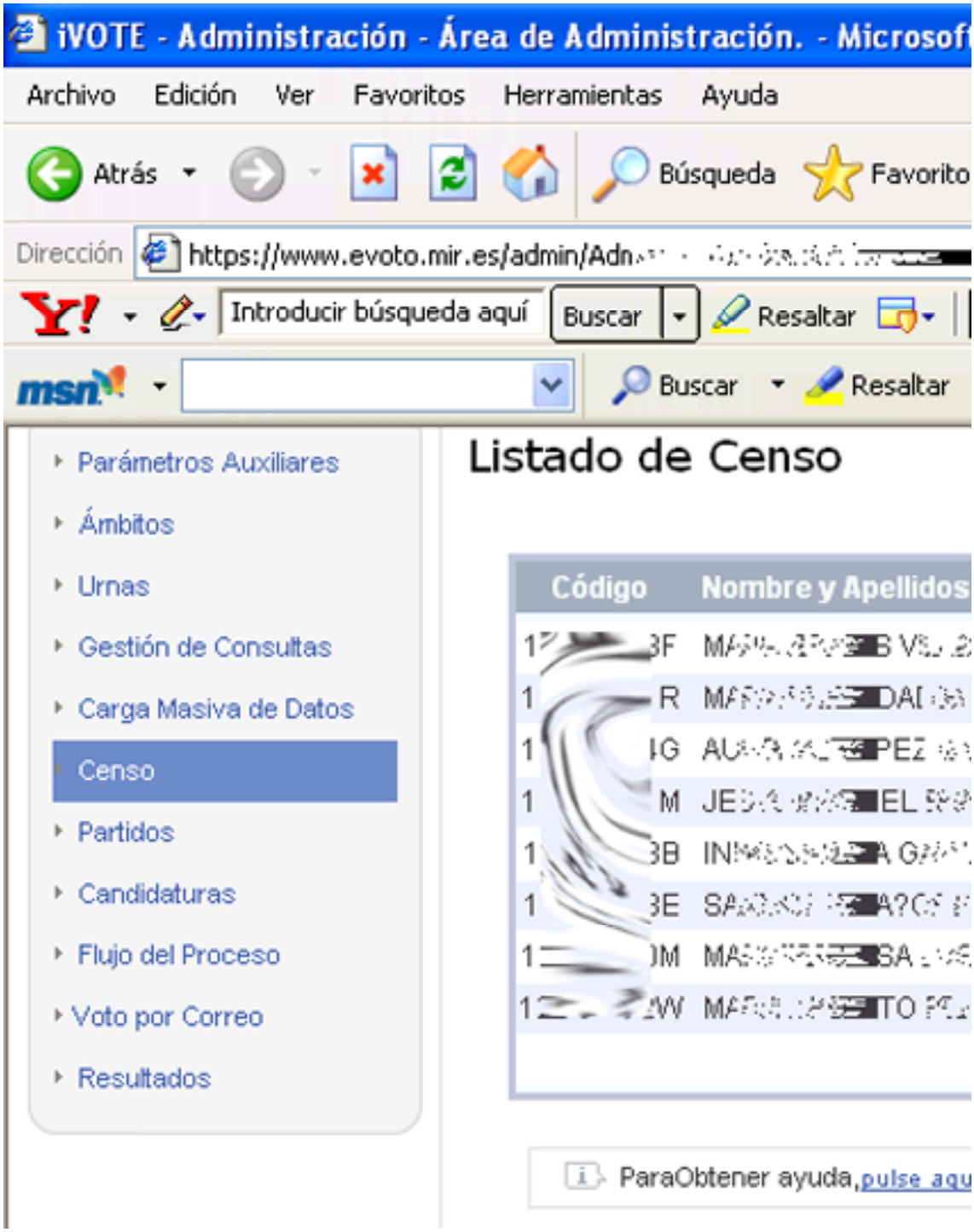
El fallo crítico que invalida el uso de ésta aplicación es que al realizarse la elección de voto desde un entorno HTML, con un formulario normal y ser lanzada la pantalla de aviso por un javascript, un programa ***malicioso*** instalado a la espera en el ordenador del votante podría ***saber*** lo que se ha votado y además ***cambiar*** el voto elegido si ese fuera el propósito.

Después que el votante pulsa en 'ACEPTAR', no vuelve a tener ninguna confirmación que su voto ha llegado al destino, ni obtiene ningún recibo, ni puede confirmar posteriormente con ningún procedimiento que su voto no ha sido manipulado.

Sólo después de pulsar 'ACEPTAR' se pasa el voto al applet Java que lo firma y codifica, pero justo en ese lugar se encuentra el punto débil del sistema. Existen mejores métodos para procesar el voto del usuario.

Fallos de seguridad muy serios

Se pudo, desde el exterior, acceder al menú de votaciones.



Acceso a los listados del censo desde el menú de votaciones. Está ofuscada la URL y los datos personales

Acceso a menú de gestión de proceso electoral

Acceso a listado de municipios

Acceso a listado de opciones

Las opciones que se encuentran en esta parte del menú son las que permiten gestionar las fases por las que pasa el proceso electoral

Para la PVI, por su importancia, por el tamaño del campo sociológico, no debieran utilizarse DNS. Es fácil controlar algunos servidores de dns en redes, como pueden ser los de cable. Con una aplicación simulada se podrían robar certificados masivamente para su uso fraudulento en la propia votación. Es la misma técnica usada por los ladrones de claves bancarias y de la que tanto hemos oído hablar en los últimos meses.

Esta técnica, conocida como 'phising', consiste en hacerse pasar por otro intentando extraer información sensible de inocentes usuarios.

Estilo apresurado

El estilo apresurado que se percibe en todo el código, es un grave error en sí mismo que genera un alud de fallos de muy fácil identificación.

Accesibilidad para Incapacitados. La aplicación utilizada no cumple los estándares de accesibilidad más elementales. Lo habitual en el trabajo para organismos públicos a nivel mundial

es utilizar al menos páginas web XHTML, con un uso adecuado de hojas de estilo CSS y el cumplimiento de normas de accesibilidad para discapacitados que cumplan con la norma americana 508 (**http://www.access-board.gov/sec508/guide/**) o bien la WAI-AA (**http://www.w3.org/WAI/WCAG1AA-Conformance**) Web Content Accessibility Guidelines.
Es lamentable comprobar como incluso algunas de las páginas ni siquiera incluyen una cabecera HTML describiendo el 'doctype' utilizado.

El CSS utilizado en la web es rancio y completamente obsoleto.
La primera página de acceso está completamente vetada para los invidentes ya que consiste únicamente en una sola fotografía.

Los invidentes utilizan unos 'lectores' que les dictan la página en la que navegan. Esos lectores, conocidos como 'screen-readers', leen en voz alta los menús de la página web para que el invidente se oriente y pueda elegir dónde quiere ir. Cuando en una página web no tenemos más que una fotografía y no hay texto que leer, el invidente no puede continuar porque no sabe lo que hay allí.

La primera página contiene únicamente la selección de idioma y un botón para continuar. ¿De verdad era necesario hacerlo así?.

Algoritmos de seguridad. La aplicación usa todavía algoritmos como el MD5, Message-Digest algorithm 5, que se saben comprometidos desde que el pasado mes de agosto (2004), un equipo de criptógrafos chinos (Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu) descubrió una vulnerabilidad que permite efectuar un ataque de duplicación en menos de una hora con la potencia de computación adecuada. http://en.wikipedia.org/wiki/MD5

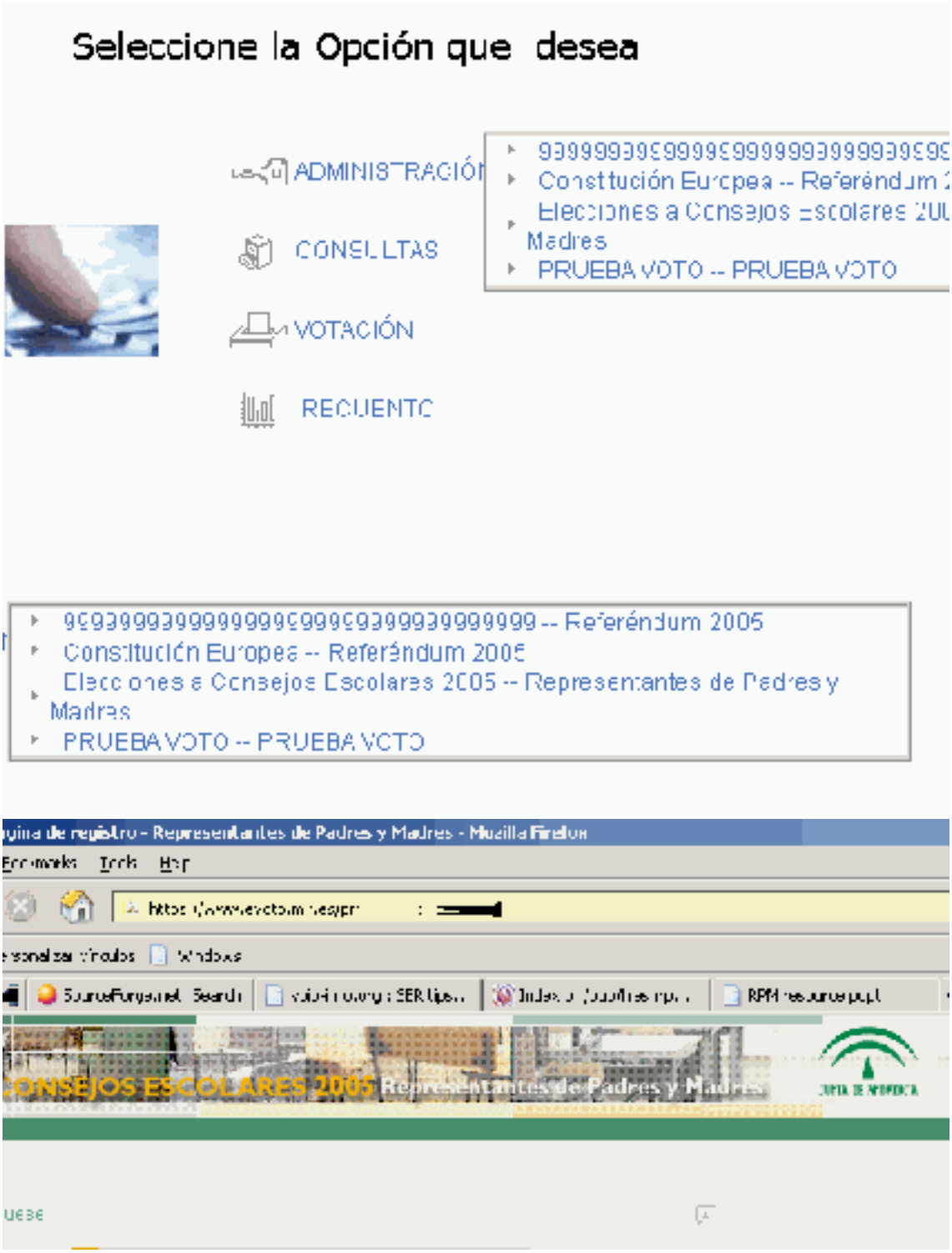
El mismo equipo ha hecho público en fechas recientes que ha conseguido rebajar considerablemente la seguridad del algoritmo SHA1 (Secure Hash Algorithm), utilizado en todos los protocolos de firma y certificación digital.
http://www.schneier.com/blog/archives/2005/02/sha1_broken.html

El mismo NIST, National Institute of Standards, de EEUU ya ha avisado hace tiempo que dejará de utilizarlo en 2010.

¿Aplicación Multiuso?

La aplicación ha sido usada también para las votaciones de la Guardia Civil y las elecciones de representantes de Padres y Madres de alumnos de Andalucía.

Entendemos perfectamente lo de la Guardia Civil, pero ¿por qué se utilizan los recursos del Ministerio del Interior para hacer las elecciones a los Consejos Escolares de Andalucía y no el Ministerio de Educación, por ejemplo?.



Pantallas del menú de la aplicación y pantalla del menú para la elección del Consejo Escolar de Andalucía

Recomendaciones para la Junta Electoral Central

El caso Indra Sistemas recuerda, por su similitud, al caso Diebold en EE UU [http://avirubin.com/vote/analysis/index.html].
Nadie deseaba y aún menos el OVE lo que ha ocurrido. En ningún momento pudimos imaginar que nos daríamos de bruces con tanta improvisación y errores de bulto de tan grueso calibre. La Junta Electoral tiene que asumir el liderazgo que la Ley le confiere para organizar con madurez el despliegue de las infraestructuras tecnológicas, que están llamando con fuerza a la puerta, así como el control de la administración electoral. No hay marcha atrás. Las tareas a realizar son muchas y el tiempo juega en contra.

Queremos recordar a la Junta Electoral que es prescriptivo, no opinable, el uso de aplicaciones de Código abierto, o como mínimo un código accesible bajo cláusula de no revelación en caso de utilizar software propietario, para que sea sometido a escrutinio público de expertos independientes. Que es prescriptivo, no opinable, que los recursos tecnológicos sean independientes de la plataforma de software y hardware del cliente para garantizar la universalidad del voto. No se debe, bajo ningún concepto, asociar voto a un único fabricante o Sistema Operativo. ¿Es imaginable un país, España, por el que circulara, exclusivamente, un único modelo de un sólo fabricante de automóviles?.

Es imprescindible, en el mismo sentido, garantizar la accesibilidad para cualquier votante. Especialmente importante en el caso de invidentes.

La Junta Electoral Central debiera considerar la apertura de un concurso internacional, coordinado con el Gobierno español, para el diseño de un nuevo sistema 'hash' que sustituya al MD5 y SHA1 como estándares habituales. Recomendamos la utilización de SHA-256 como punto de partida para una base segura en estos momentos.

Conformidad con Estándares Internacionales. Recomendamos la lectura atenta de las recomendaciones legales y técnicas del Consejo de Europa sobre voto electrónico, disponible desde el 05/10/04 en nuestra propia web [**http://www.votobit.org/lallave/consejo1.html**]. No son punto y final o la meta, nada de eso, pero constituyen un punto de partida necesario para familiarizarse con las nuevas infraestructuras y las obligaciones que se derivan de su despliegue.

Créditos. OVE (Observatorio Voto Electrónico). **COORDINADOR**: Luis Panizo, **ANALISTAS**: Jorge García (Arquitectura), Juan Antonio Martínez (Código), Jorge Valencia y José Manuel Guerrero (Auditoría de seguridad), Antonio Yuste (Relator).