Fraude Electoral y Sistemas Automatizados

Por: Carlos E. Soucre

“Las máquinas no separan al hombre de los grandes problemas de la naturaleza, más bien, lo sumergen más en ellos”

Antoine de St. Exupery

Introducción

El objetivo esencial de una elección es permitir que la sociedad exprese sus preferencias de cómo y por quién deben ser gobernados. Naturalmente la integridad del proceso electoral es fundamental para la integridad de la democracia en sí misma. El proceso de ejecución de una elección es tan importante como la tecnología sobre la cual está fundamentada, debe ser resistente a la manipulación, de modo de frustrar un amplio espectro de ataques entre los cuales se incluye el voto múltiple, por parte de los electores, o la incorrecta totalización por parte de personas inescrupulosas, que pueden formar parte de las autoridades electorales. La historia está plagada de ejemplos de elecciones que han sido manipuladas para alterar los resultados.

Dado que, por su naturaleza electrónica, los votos digitales no son auditables, el sistema electoral debe ser adecuadamente robusto para soportar una gran variedad de comportamientos fraudulentos e, igualmente, debe ser transparente y lo suficientemente comprensible para que el público y los candidatos puedan aceptar los resultados.

El diseño de un “sistema electoral”, bien sea electrónico o manual (tradicional), debe satisfacer un número de criterios que, en muchos casos, pueden ser antagónicos. Ninguna tecnología de punta puede reparar un proceso fundamentalmente viciado; es necesario que existan políticas adecuadas y que se involucre a diversas instituciones tanto gubernamentales como ONGs y a la sociedad civil para que cualquier sistema electoral sea implementado correctamente. La participación parcial o coaccionada de esos actores permite la realización de un fraude.

A continuación, se exponen los aspectos fundamentales que conforman la aplicación de la plataforma tecnológica para un proceso electoral y las fallas que pueden ser explotadas para cometer fraude comicial.

1. Sistemas Electorales Automatizados.

Se han hecho múltiples estudios para la implementación de tecnologías informáticas con la finalidad de optimizar y agilizar los procesos electorales y, en su gran mayoría, se advierte sobre los riesgos que acarrea la implementación precipitada de una plataforma electoral, debido a los desafíos en la ingeniería del software, las amenazas internas, las vulnerabilidades en las redes de computadoras y los problemas de auditoria. Pero el problema fundamental, en un sistema electoral electrónico, es que la totalidad del sufragio electoral depende de la robustez, la exactitud y de la seguridad, tanto en las máquinas de votación como en los sistemas de transmisión y totalización.

En toda tecnología electrónica, particularmente en las tecnologías de seguridad informática, el factor humano es un componente crítico.

En la misma medida en que los avances tecnológicos son integrados cada vez más en los procesos electorales, la estandarización comicial debe ser precisa y oportunamente fundamentada por las autoridades electorales, con la participación de expertos calificados en, sistemas de información, seguridad informática, redes y telecomunicaciones. Los estándares de votación deben ser abiertos, seguros e implementables; de modo que cualquier organización competente pueda desarrollar un sistema electoral compilante. Esto, además de garantizar un mercado competitivo para las empresas proveedoras de sistemas electorales, ayuda a mejorar la percepción y la confianza del público hacia los sistemas electorales automatizados.

Ninguna tecnología de punta es capaz de resolver todos los problemas o mitigar todos los riesgos. Ningún sistema de votación, bien sea electrónico o manual, es una panacea. Un sistema electoral ideal es aquel que resume los mejores atributos y beneficios de ambos métodos de votación y emplea una construcción modular que permite, en forma sencilla, la integración de los procedimientos manuales y las tecnologías digitales; siempre y cuando se eviten las consecuencias inherentes a la dependencia de una de las dos técnicas en particular. La implementación mal concebida de un sistema híbrido, en lugar de ventajas, puede presentar los problemas propios de ambos métodos electorales.

El diseño de un sistema de votación es un reto particularmente difícil, ya que el voto debe ser secreto. Las auditorias en los sistemas de transacciones digitales, usualmente se implementan registrando los datos en un sistema de identificación (como una cuenta bancaria o una tarjeta de crédito) y emitiendo recibos. Los sistemas de votación híbridos, al imprimir un registro anónimo de cada voto, donde el elector pueda verificar que su voto ha sido correctamente emitido por el sistema, antes de depositarlo obligatoriamente en una urna, brindan la posibilidad de crear un registro físicamente auditable.

Los votos impresos en papel, conforman la única evidencia física auditable en caso de requerirse un reconteo para verificar la emisión de votos para cada opción

Tal como se ha hecho hincapié anteriormente, la auditabilidad es un componente crucial en todo proceso electoral; los sistemas electrónicos, aun siendo capaces de registrar cada voto emitido en todos los centros de votación, sólo representan un método rápido y eficiente de escrutinio para proveer los resultados de una elección, pero por su naturaleza, los votos digitales no son auditables.

Para que una auditoria pruebe ser significativa, es preciso que todos los votos emitidos por las máquinas electorales, sean depositados en urnas electorales capaces de resistir posibles violaciones y que éstas sean debidamente manejadas y custodiadas. Adicionalmente, como los votos físicos pueden ser contados a mano, el uso de máquinas o sistemas mecánicos de conteo no es indispensable en una auditoria.

Un buen sistema electoral requiere de un buen estándar de diseño.

La tecnología no siempre es neutral; la operación de los sistemas tecnológicos suele estar influenciada por valores o intereses humanos, los cuales pueden ser embebidos dentro del diseño de todo el sistema, especialmente cuando no se establecen rigurosos estándares de diseño ni se implementan estrictos procesos de revisión. Estos valores o intereses pueden ser directos (cuando se excluye a los votantes con necesidades especiales o discapacidades) o persuasivos (cuando la selección de un voto se hace mas fácil que otro). En ocasiones, pueden ser no intencionales, cuando, por ejemplo, se genera una propensión directa, si en el diseño de las máquinas electorales no se contempla un método alternativo para la selección del voto activado por voz para los electores invidentes.

Las revisiones y auditorias del sistema deben ser realizadas en al menos tres escenarios distintos:

1. Los prototipos del sistema deben ser rigurosamente inspeccionados y analizados con la finalidad de constatar que cumplen con los estándares y las especificaciones de diseño originales, además de garantizar que los equipos funcionen correctamente.

2. Se debe determinar que las máquinas que finalmente serán distribuidas en los centros de votación son exactamente iguales al prototipo requisado previamente y que cualquier aditamento posterior en el equipo o modificación del software, no viole las especificaciones y estándares aprobados.

3. Finalmente, los equipos de votación deben ser certificados para que puedan ser efectivamente preparados y calibrados, de modo que todas sus funciones operen correctamente, según lo especificado.

Mas allá de las paredes de un laboratorio o un centro de votación, estos sistemas deben ser probados en público, por los propios votantes que los usarán el día de los comicios; para tal fin, el sistema de votación podría perfectamente ser empleado para la elección de las autoridades estudiantiles en cualquiera de las universidades nacionales o podría ser desplegado en diversos lugares públicos en todo el país (tales como alcaldías, gobernaciones o dependencias gubernamentales), para la realización de consultas de opinión sobre cualquier asunto de interés público.

Pese a la posibilidad de que cada voto depositado puede ser auditado, es fundamental que el sistema sea sometido a una serie de pruebas intensivas para determinar los niveles de seguridad, funcionalidad y confiabilidad de todo el sistema electoral.

Estas pruebas proporcionan el beneficio combinado de sensibilizar y familiarizar al público con la nueva tecnología y de someter al sistema de votación a rigores y condiciones similares a los comicios reales; certificando que éste trabajará adecuadamente y será capaz de proporcionar a los usuarios de una interfaz sencilla y utilizable.

Una elección legítima avala que todos los votos contados son los mismos votos introducidos por los votantes.

Si existe alguna duda sobre la realización de los comicios electorales, entonces los resultados deben ser sometidos a un examen minucioso. La auditoria final del proceso electoral, además del recuento de los votos depositados en las urnas y el proceso en sí, debe abarcar todo el sistema electoral, ya que muchas de las irregularidades pueden ser directamente relacionadas con las debilidades y fallas del sistema.

En la eventual asistencia del sector privado a las autoridades electorales para la auditoria del sistema electoral, no se deberá involucrar a los desarrolladores del sistema ni a ninguna empresa relacionada. Un examen de la totalidad de la plataforma tecnológica por parte de terceros puede ayudar a minimizar las oportunidades de manipulaciones por parte de parcialidades y/o sabotajes.

El proceso de auditoria, debe ser cabal para avalar la legitimidad de los resultados y por su carácter vinculante, debe ser aceptado por las partes involucradas.

Las pruebas del sistema son necesarias pero no son suficientes para un exitoso proceso electoral; se pueden omitir ciertos factores o interacciones, que en muchos casos pueden ser fácilmente detectables por medio de la simple observación. La interacción entre los sistemas puede ser impredecible así como también resulta imposible predecir el factor humano, bien sea debido a simples errores o a manipulaciones intencionales. Las pruebas son esenciales, sin importar el tipo de sistema. Una auditoria final sobre el sistema electoral puede corroborar la validez de las pruebas realizadas. Al igual que las pruebas que se ejecuten sobre el sistema antes de una elección, no garantizan la exactitud del escrutinio final. Las auditorias finales no evalúan la utilidad del sistema.

2. Sistemas Electorales Certificados.

Para la adopción de un sistema de votación electoral es importante que previamente se realicen evaluaciones y estudios de factibilidad independientes; pero para que exista una verdadera transparencia en el proceso de adquisición e implementación de un Sistema Electoral Automatizado con una tecnología especifica, es imperativo que todo el sistema de votación y totalización sea inspeccionado minuciosamente; se debe comprobar su exactitud e integridad, así como también la seguridad y la capacidad del sistema para ser auditado. Para garantizar a los electores la validez y privacidad de su voto individual, se requiere algo más que los alegatos de los expertos electorales y los proveedores del sistema de votación. Los recursos y métodos del Sistema Electoral Automatizado deben ser realmente transparentes: los votantes podrán acceder fácilmente a estudios, resultados de pruebas de evaluación, información concerniente al desempeño del sistema en otros comicios (locales, nacionales o extranjeros) y a cualquier otro tipo de información relevante acerca de la tecnología electoral, empleada en el sistema al cual confiarán su voto el día de las elecciones.

La transparencia y la privacidad son dos componentes vitales para el éxito de cualquier Sistema Electoral Automatizado; sin ellos el sistema y la democracia sucumben.

Si el software o la mecánica subyacente al Sistema Electoral Automatizado no son del dominio público, al menos estos deben estar disponibles para ser analizados por expertos calificados de diversas disciplinas en el campo de la informática. Un proceso que haya sido amplia y abiertamente supervisado tendrá un mayor grado de legitimidad que otro cerrado; igualmente, los códigos "abiertos" permiten una verdadera transparencia en los procesos digitales. Si el código fuente del Sistema Electoral Automatizado está protegido por las leyes internacionales de propiedad intelectual o algún tipo de acuerdo de privacidad (*Nondisclosure Agreement*), obtener acceso a éste es un problema añadido, debido a que tales prácticas restrictivas coartan su evaluación —lo cual resulta inaceptable en el ámbito del sufragio. Por esta razón, entre otras, los programas de código abierto son ideales para ser usados en cualquier sistema que procese, cuente y totalice votos. La exposición del código fuente puede servir para que los proveedores elaboren mejores aplicaciones. Las reservas legales realmente no tienen ninguna cabida en ningún Sistema Electoral Automatizado

Comúnmente, los proveedores de sistemas que requieren un elevado nivel de seguridad y confiabilidad, como los sistemas de votación electrónicos, defienden la tesis de la "seguridad mediante la oscuridad" como el mejor método de protección. Esta teoría puede tener cierta validez, pero la verdad es que ocultar las fallas de seguridad nunca ha sido una estrategia de seguridad consistente. Universalmente, los expertos en seguridad coinciden en lo inadecuado que resulta la "oscuridad" para proveer algún tipo de protección significativa, ya que no considera las necesidades integrales de seguridad del sistema completo.

Un exhaustivo análisis del código del software y de las diversas tecnologías que integran el sistema de votación digital, donde se incluya a todas las partes involucradas en el proceso electoral, no garantiza que éste pueda ser totalmente seguro —esto es imposible—, pero incrementa la posibilidad de descubrir las fallas de seguridad relevantes en el Sistema Electoral, que puedan ser explotadas tanto por personas ajenas al sistema (votantes inescrupulosos, rivales electorales), como por agentes internos (funcionarios electorales, desarrolladores del sistema). Dado que un atacante resuelto puede a la par estar buscando las debilidades del sistema, para introducir deficiencias o tomar ventaja de cualquier falla preexistente, es necesario, en el interés público, que las autoridades electorales encuentren las brechas de seguridad primero y éstas sean inmediatamente reparadas por el proveedor del sistema electoral, sobre quien recae finalmente toda la responsabilidad referente a la seguridad del Sistema Electoral Automatizado.

3. Impresiones sobre el Sistema Electoral Automatizado

El Consejo Nacional Electoral (CNE), que es la autoridad electoral venezolana, ha adoptado e implementado hasta la fecha dos Sistemas Electorales Automatizados y, aparentemente, en ninguno de los dos casos ha cuestionado críticamente las especificaciones de seguridad y confiabilidad que declaran los proveedores de los sistemas; no ha reparado en las objeciones hechas por expertos e instituciones; ni ha considerado las consecuencias de su propia ignorancia y ligereza al empeñarse en acoger una tecnología específica, bien porque hayan tomado como premisa sus predisposiciones y expectativas personales o porque hayan estado sometidos a la influencia ejercida por el proveedor del sistema, fuente primaria de información disponible.

El sistema implementado actualmente por el CNE fue dudosamente "certificado" para su uso, sin ningún tipo de informe público que respaldase los análisis de certificación; ni mucho menos hubo publicación de ningún aspecto del "código fuente" del sistema electoral, que pudiera permitir un examen por parte de una organización independiente.

Dada la dificultad que existe en mantener la integridad de la data electoral a través de una inmensa red de equipos y sistemas, de modo de poder producir y garantizar un resultado claro, perfectamente aceptable por cualquiera de las partes involucradas en un proceso comicial;

cabe preguntar, ¿cómo puede una empresa desarrollar un sistema electoral con un enfoque de "caja negra", sin tomar en consideración el resto del sistema? La respuesta a esta pregunta puede ayudar a explicar muchos de los problemas concernientes a la seguridad del actual sistema electoral y a aspectos tan simples como la pesadilla de la interfase para los usuarios

Básicamente una "caja negra" es una solución sencilla, fácil de usar e integrar (p.ej.: en una red cliente-servidor). Ésta interactúa con el mundo exterior a través de un mecanismo relativamente pequeño y simple, cuyos parámetros de ejecución han sido muy bien definidos de modo que todos los detalles concernientes a cómo el resultado deseado es obtenido, permanecen herméticamente ocultos en su interior. Una aplicación podría ser una posible sistematización maliciosa envuelta en un bonito empaque, lista para adecuarse transparentemente a cualquier código.

El punto fundamental con las "cajas negras" es que son opacas; su funcionamiento interno no es perceptible; y, básicamente, son definidas de acuerdo a su función como parte natural de una estructura delegada y por el resultado que producen; por ejemplo, la máquina electoral Smartmatic SAES3000.

Normalmente existen muchas complejidades y detalles relacionados con la implementación de una "caja negra" como parte de un sistema electoral digital, las cuales no deberían formar parte de su desarrollo y diseño; sólo debe existir una relación clara entre la entrada y la salida, por lo que sólo deberían requerir estrictamente los datos necesarios para computar un resultado.

Dado los antecedentes previos a la celebración de los comicios refrendarios y a la falta de información, podemos especular seriamente acerca de las fallas ocultas del sistema electoral y sus alcances, o de la disciplina de desarrollo y la calidad de la ingeniería del software en general. Lo cierto es que no existe ninguna evidencia que indique la existencia de algún tipo de control de cambios de procesos, el cual pueda limitar la capacidad de que algún desarrollador introduzca vulnerabilidades en el código, que pudieran ser explotadas posteriormente, ni tampoco de la existencia de métodos criptográficos y de la forma en que fueran utilizados.

Lo anterior nos permite asumir que:

- Trabajadores electorales con alguna parcialidad, con acceso a las máquinas de votación Smartmatic SAES3000 (las que serán denominadas en lo sucesivo como "terminales electorales"), antes del proceso electoral, pueden haber ejecutado acciones administrativas sobre el programa del terminal.
- Las técnicas criptográficas empleadas en los protocolos para la comunicación del terminal electoral con el servidor central –bien sea para obtener información para la configuración de la elección o para enviar el reporte final de la votación–, puede que no sean correctas o no existan.
- No se implementaron mecanismos para verificar la integridad de los datos transmitidos entre terminales electorales y el servidor central.

Lo que da cabida a la posibilidad de que el sistema sea vulnerable a ataques "sin trazas", tales como la introducción de un "buffer overflow" (rebose de la memoria) en los terminales de votación, o a que la ejecución de un ataque tipo "man-in-the-middle" (hombre en el medio) al sistema en general, sean muy altas.

Cabe aclarar que la introducción de un ataque con algún virus informático resulta ilógico, ya que si se asume que se desconoce la naturaleza del sistema sobre el cual corre el software en los terminales electorales, no se sabe con certeza qué tipo de debilidad en el código se debe explotar.

La intención de un ataque a un proceso electoral por lo general tiene la finalidad de modificar los resultados finales.

4. Los ataques al Sistema Electoral

En los sistemas electorales, proteger la integridad y privacidad de la data critica, i.e. la configuración de la votación, los votos, los resultados, etc., es indudablemente muy importante. Existen dos vectores principales para acceder y atacar la data del sistema electoral: mediante el acceso directo a la memoria del terminal de votación y a través de una conexión de red; ambos métodos, sumamente efectivos y furtivos.

Cada terminal de votación tiene dos tipos distintos de almacenamiento interno. El primero, o área principal fija, almacena el sistema operativo del terminal, los programas ejecutables y la información de la configuración del sistema, entre otros y el segundo, o área de memoria de almacenamiento, donde se almacenan los datos dinámicos, como los registros de la votación.

Los terminales electorales no pueden trabajar aisladamente; deben ser capaces de recibir datos referentes a la configuración de la elección (entrada) y enviar el reporte de los resultados de la votación (salida). Ambos procesos de entrada y salida de datos se realizan directamente con la autoridad electoral a través de una conexión de red.

Una vez concluido el proceso electoral, los resultados de los terminales electorales son enviados a un servidor principal para su escrutinio final. Lo que no está claro es si estos reportes deben ser considerados como resultados preliminares u oficiales.

4.1. Manipulación de la configuración del sistema

Cada terminal electoral debe mantener el récord del número total de votos que han sido sufragados en un "contador de seguridad", el cual puede consistir en un simple archivo mutable. Si este archivo es modificado dentro de un terminal, un adversario puede generar dudas, creando una discrepancia entre el número de votos sufragados en ese terminal y la totalidad de los votos escrutados. Aun si se implementase un conteo del número de bits o "checksum" encriptado, esto no sería suficiente para proteger al contador de seguridad. Un atacante con la habilidad de ver y modificar el archivo todavía sería capaz de llevar el contador a un estadio anterior. De hecho, la única solución que podría funcionar es la implementación del contador de seguridad en un dispositivo de seguridad adosado al hardware del terminal (lo que implicaría una serie de modificaciones del mismo y elevaría considerablemente los costos).

4.2. Manipulación de la configuración del terminal de votación

Dentro del terminal electoral existe un archivo con la "configuración de la elección", que contiene todo lo concerniente a la forma específica en que operará el terminal, desde la información acerca de las opciones electorales y sus asignaciones, hasta el nombre del usuario y la clave de acceso que serán usados cuando el terminal reporte los resultados. Estos datos no necesariamente deben ser cifrados o su checksum debe ser verificado en el momento de configurar el terminal electoral antes de la votación o, en una escala mayor, a través de una conexión de red. Un intruso, incluso sin conocer la estructura exacta de la "configuración del sistema", puede agregar, eliminar e incluso modificar las asignaciones de la votación, confundiendo los resultados y, en consecuencia, alterar el archivo que almacena los resultados; por ejemplo, los votantes podrían ver las opciones correctas en el sistema e inocentemente votar por la opción contraria, pese a que el comprobante refleje la opción correcta (he aquí la importancia del correcto manejo y custodia de las urnas electorales). La información referente a las opciones electorales en sí, no son reflejadas en los resultados, sólo se indica que la opción "1" obtuvo una cantidad de votos y la opción "2" obtuvo otra cantidad.

4.3. Usurpación de terminales de votación legítimos.

Los terminales electorales están configurados para que al finalizar la elección, a través de un acceso telefónico, transmitan los votos totalizados a un servidor central, donde serán tabulados. Un intruso capaz de engañar al servidor central, simulando ser un terminal legítimo, obviamente podría causar daño al proceso electoral, reportando resultados falsos al sistema de totalización. Todos los datos requeridos para que el terminal se comunique con el servidor, como el número para el acceso PPP, el nombre del usuario, la clave de acceso y la dirección

IP del servidor central, el número de serial del terminal, etc. –como es bien sabido– están almacenados dentro de cada terminal en un archivo de configuración y son fácilmente accesibles por parte del personal interno de cada centro de votación. Esto genera un vector para que un intruso pueda conocer casi todo lo necesario para acometer su objetivo.

4.4. Manejo de los aspectos criptográficos.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en las comunicación entre dos miembros de una red; en segundo lugar, asegurar que la información que se envía es auténtica, que la misma sea recibida exclusivamente por el destinatario y, por último, impedir que el contenido del mensaje enviado (habitualmente denominado criptograma) sea modificado en su tránsito.

En esta sección trataremos de sumariar los aspectos más resaltantes en el uso de la criptografía para proteger la data electoral y los registros de auditoria de los terminales electorales, para luego continuar con las consecuencias de una pobre implementación.

a) **Manejo de las claves digitales.**
   Toda la data critica, almacenada en el terminal, puede que sea cifrada mediante el uso de un Algoritmo Simple de Cifrado Simétrico, incluido dentro del código fuente del terminal. A diferencia de los sistemas de cifrado asimétricos, aquellos funcionan más rápido y ocupan menos espacio (lo cual es conveniente, dada la simplicidad del terminal electoral). El principal problema con los sistemas de cifrado simétrico no está ligado a su seguridad sino al intercambio de claves. Si el atacante tiene acceso a una parte del código fuente usado en los terminales electorales, o intercepta una clave, entonces puede fácilmente leer y modificar los registros de votación y auditoria.

b) **Cifrado**
   Aun si se implementase correctamente un sistema de cifrado basado en hardware, las claves generadas por medio de un cifrado simétrico pueden ser recuperadas mediante un método de “fuerza bruta” en un periodo muy corto de tiempo, por lo que se debería reemplazar el método de cifrado por uno asimétrico preferiblemente.

c) **Verificación del mensaje o Firma Digital**
   La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático (conjunto finito de instrucciones o pasos que sirven para ejecutar una tarea o resolver un problema) matemático, denominado función hash, a su contenido. Esta función asocia un valor dentro de un conjunto finito, generalmente los números naturales, a su entrada. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante esto presenta algunas dificultades.
   Para que sea de utilidad, la función hash debe satisfacer dos importantes requisitos. Primero, debe ser difícil encontrar dos documentos cuyo valor para la función "hash" sea idéntico, cosa que resulta aún más difícil si el mismo algoritmo se usa en todos los terminales electorales por estar incluido en el código fuente. Segundo, una vez encriptado el documento, debería ser imposible recuperar el original.
   Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. El firmante cifra el documento con su clave privada y cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrarla.
   Existen funciones "hash" específicamente designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos. Para usarlos, un documento se firma con una función "hash", cuyo resultado es la firma. Otra persona puede comprobar la firma aplicando la misma función a su copia del documento y comparando el resultado con el del documento original. Si concuerdan, es casi seguro que los documentos son idénticos.
   Lo importante es utilizar una función "hash" para firmas digitales que no permita que un "atacante" interfiera en la comprobación de la firma. Si el documento y la firma se enviaran descifrados, este individuo podría modificar el documento y generar una firma

correspondiente sin que lo supiera el destinatario. Si sólo se cifrara el documento, un atacante podría manipular la firma y hacer que la comprobación de ésta fallara. Una tercera opción es usar un sistema de cifrado híbrido para cifrar tanto la firma como el documento. El firmante usa su clave pública y cualquiera puede usar la misma clave pública para comprobar la firma y el documento. Esto suena bien pero en realidad no tiene sentido. Si este algoritmo hiciera el documento seguro también lo aseguraría contra manipulaciones y no habría necesidad de firmarlo. El problema más serio es que esto no protege de manipulaciones ni a la firma, ni al documento. Con este método, sólo la clave de sesión del sistema de cifrado simétrico es cifrada usando la clave privada del firmante. Cualquiera puede usar la clave pública y recuperar la clave de sesión. Por lo tanto, resulta obvio usarla para cifrar documentos substitutos y firmas, para enviarlas a terceros en nombre del remitente.
Un algoritmo efectivo debe hacer uso de un sistema de clave pública para cifrar sólo la firma. En particular, el valor "hash" se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado. Si el documento se modifica, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone debe descubrir.

4.5. Manipulación de los resultados electorales

Objetivos ideales para un ataque son los registros de los votos en sí. Cuando éstos son almacenados en un dispositivo pueden ser cifrados (especialmente si los votos son transmitidos al servidor central usando una conexión telefónica), lo que minimiza el riesgo de un ataque, pero no sus consecuencias.

En la sección 4.2 se describe cómo un adversario podría alterar la configuración de la elección en el terminal electoral, y en la sección 4.3 se establece la posibilidad de introducir votos falsos en el servidor central, mediante la usurpación de la identidad de los terminales de votación. A continuación se describe otra forma de modificar los resultados de la elección, modificando el registro de votación almacenado en cada terminal electoral. Gracias a una pobre implementación de los métodos criptográficos descritos en el punto anterior; un atacante con acceso a este archivo podría generar o cambiar los resultados a voluntad, sin dejar ningún tipo de evidencia (al contrario de los ataques descritos en los puntos 4.2 y 4.3). Si las conexiones desde los terminales electorales con el servidor central son concentradas y redirigidas a través de un enlace de red desde la empresa telefónica hasta la autoridad electoral, entonces se genera un nuevo vector, donde podría actuar una parcialidad con la capacidad de operar dentro de la red de comunicaciones y en complicidad con la autoridad electoral para tomar ventaja sobre la otra.

Mediante la implementación de un ataque similar al del “man-in-the-middle” o TCP Hijacking, que consiste básicamente en la intercepción de los paquetes de datos de una red para ser modificados y posteriormente reinsertados en la red, se puede modificar en forma controlada los resultados transmitidos desde los terminales (p.ej.: sustrayendo una cantidad de votos a una opción para sumarlos a la otra, de acuerdo a un criterio especifico). Para la ejecución de una agresión de estas características, el atacante debe estar en conocimiento de la estructura del protocolo empleado en la comunicación entre los terminales electorales y el servidor central, y debe tener la capacidad de montar una infraestructura adecuada para el manejo de datos en forma intensiva (la cual podría funcionar bajo la fachada de algún dispositivo anexo, vinculado con el proceso electoral). Esta manipulación puede ser detectada si se compara la data almacenada en los terminales electorales con la data transmitida pero, como se describe anteriormente, los datos almacenados dentro de cada terminal pueden haber sido sujetos a modificaciones. Por último, cabe aclarar que este tipo de ataque puede ser evitado mediante el uso de herramientas criptográficas asimétricas estándar, como el SSL (Secure Socket Layer) o Capa de Conexión Segura, también conocido como TLS, según el estándar del “Internet Engineering Task Force”.

5. Conclusión

En resumen:

- Ninguna tecnología de punta puede reparar un proceso fundamentalmente viciado
- Por su naturaleza, los votos digitales no son auditables.
- El funcionamiento interno de una "caja negra" no es perceptible.
- Existen vectores efectivos para acceder y atacar la data del sistema electoral.
- Se puede engañar al servidor central, reportando resultados falsos al sistema de totalización.
- Los mensajes cifrados pueden ser modificados en transito
- Implementando un ataque del tipo "man-in-the-middle" (hombre en el medio), se puede modificar efectivamente en forma controlada los resultados transmitidos desde los terminales.

Se puede concluir que el sistema desarrollado (en un breve periodo de tiempo) por el consorcio SBC-Smartmatic, ofrecido bajo el esquema de "caja negra" y cuya única pieza visible o, mejor dicho, conocida es un "terminal electoral" (el cual fue desarrollado originalmente por la empresa italiana Olivetti Tecnost, como parte de una solución "llave en mano" para la implementación de terminales de loterías denominada Olivetti Gaming Ware), no ofrece ningún indicio claro de que un nivel de disciplina de programación y un mínimo control de calidad en los procesos, para un proyecto de esta envergadura, hayan sido observados. Tampoco se evidencia que la naturaleza oscura y secreta del sistema electoral de la empresa Smartmatic, realmente garantice los elevados niveles de seguridad requeridos para un sistema electoral, donde la privacidad y la confiabilidad son claves para el éxito del proceso.

No se deben disfrazar las tecnologías establecidas como nuevas. Éstas sirven para lidiar con las mismas necesidades pero con mayor eficiencia o en forma diferente. Si se trata de manejar un problema sin un enfoque general y holístico, integrado con seguridad, se fracasará vilmente.

Si se piensa que la tecnología digital es la panacea para resolver los problemas electorales, entonces no se entienden los problemas ni tampoco la tecnología. La automatización por sí sola, no puede mejorar el proceso electoral. Tanto los desarrolladores como los compradores de sistemas electorales deben estar concientes de sus limitaciones intrínsecas, atentos a las conflictivas necesidades de privacidad, auditabilidad y seguridad del proceso electoral al pretender implementar soluciones encajonadas.

El modelo en el cual el proveedor desarrolla y patenta su propio código para ejecutar "nuestras elecciones" no es confiable. Si no cambiamos el proceso de diseño de nuestro propio sistema de votación por uno abierto, donde se involucren científicos, expertos calificados en sistemas informáticos, organizaciones políticas y ONGs, además de las autoridades electorales, nunca en el futuro se tendrá la certeza de que los resultados electorales reflejarán la voluntad de los votantes.

Por nuestro futuro y por nosotros mismos, debemos tener un sistema electoral confiable y robusto, para así preservar el pilar fundamental de nuestra democracia.

Carlos E. Soucre O.
soucre@hotmail.com