ARTÍCULO

ISSN 1994-5272

Amenazas y vulnerabilidades de los sistemas de voto electrónico remoto

Víctor Manuel Morales Rocha
<victor.morales@uacj.mx>
Universidad Autónoma de Ciudad Juárez

[Resumen] Los sistemas de voto electrónico remoto ofrecen ventajas importantes para los votantes. Estos deben satisfacer, al igual que cualquier sistema de votación empleado, algunas características de seguridad que garanticen la integridad de una elección. El cubrir dichas características no siempre es fácil, ya que aun cuando se dispone de técnicas y mecanismos robustos de seguridad, existen factores que pueden poner en riesgo una elección. Estos factores frecuentemente son derivados de acciones humanas, accidentales o intencionadas. Este trabajo describe los requisitos de seguridad que debería cumplir un sistema de voto electrónico remoto. Posteriormente, se presenta las principales amenazas y vulnerabilidades asociadas a este tipo de sistemas, las cuales deben ser consideradas antes de implementarse el voto electrónico remoto en cualquier elección.

[Palabras clave] Voto electrónico, voto remoto, amenaza de seguridad, sistema de votación

[Title] Threats and vulnerabilities of remote electronic voting systems

[Abstract] The remote electronic voting systems offer significant advantages for voters. These systems must require, like any voting system used, some safety features that ensure the integrity of an election. Covering these features is not always easy because even when techniques and robust security mechanisms are available. These factors are often derived from, accidental or intentional, human actions. This paper describes the safety requirements to be met by a system of remote electronic voting; then it features the main threats and vulnerabilities associated with these systems, which should be considered prior to implementation of remote electronic voting in any election.

[Keywords] Remote electronic voting, remote voting, security threat, voting system

Morales, Víctor. «Amenazas y vulnerabilidades de los sistemas de voto electrónico remoto». En: *Elecciones*, 2014, enero-diciembre, vol. 13, N.º 14, pp. 119-136

[Recibido] 01/09/14 & [Aceptado] 25/11/2014

© Oficina Nacional de Procesos Electorales

¿Por qué el voto remoto?

El propósito principal de los sistemas de voto remoto es proporcionar un medio de votación a los ciudadanos que no tienen la posibilidad de acudir a votar el día de la elección. Las razones de no poder acudir a votar pueden ser variadas. Por ejemplo, los votantes que residen en el extranjero o aquellos que viven en zonas muy alejadas a un recinto de votación.

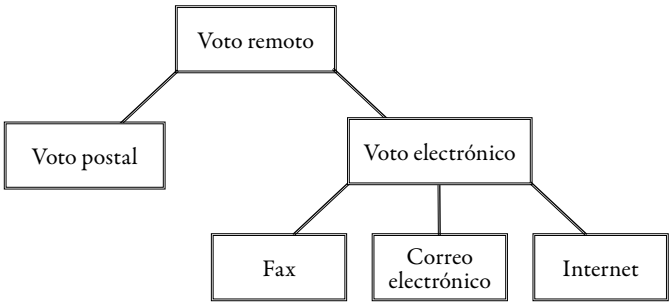
Algunos países han implementado el uso del voto postal para permitir a los ciudadanos emitir su voto de una manera remota. Sin embargo, es común que se presenten problemas de tiempo para enviar el material a los votantes, así como para recibir el voto. Aunado a eso, es muy difícil otorgar la seguridad que un voto requiere. Por esta razón, las autoridades electorales se han visto en la necesidad de estudiar vías alternas de votación remota, especialmente a través de medios electrónicos. En algunos casos, ya se han estado implementando sistemas electrónicos de votación remota, por ejemplo, en Estados Unidos (Álvarez 2007), Suiza (Republique Et Canton de Geneve 2008), Reino Unido (U.K. Pilot Schemes 2007) o Estonia (Estonian Internet Voting 2005).

En términos generales, el voto electrónico remoto puede resultar más conveniente que el voto postal. Por ejemplo, los votantes tienen menos restricciones en cuanto al tiempo en que deben enviar su voto. Además, un votante puede verificar de una manera rápida, incluso en tiempo real, si su voto ha sido recibido por la autoridad electoral. Por otro lado, en algunos sistemas, como el voto por Internet, el votante es alertado si no completa de manera correcta la selección de un voto, lo cual evita errores involuntarios que en el caso del voto en papel anularían el sufragio. A pesar de dichas ventajas, la preocupación acerca de la seguridad en los medios electrónicos de votación ha evitado que su adopción se lleve a cabo de una manera más extensa.

La figura 1 muestra una clasificación de los sistemas remotos de votación. El voto electrónico remoto no se limita a los tres medios descritos en la figura. Sin embargo, se puede considerar que son o han sido los más importantes.

 © Oficina Nacional de Procesos Electorales

Figura 1
Clasificación de los sistemas de voto remoto



Cabe resaltar que las desventajas principales de cualquier sistema remoto de votación son los riesgos de violación de la privacidad y la posibilidad de coerción o venta de votos, sin importar si el sistema se basa en papeletas (voto postal) o en medios electrónicos de transmisión (Krimmer & Volkamer 2005).

Requisitos de seguridad

Los sistemas de voto electrónico remoto deben satisfacer al menos los mismos requisitos de seguridad propios de los sistemas electrónicos presenciales, incluso los de los sistemas de voto basado en papel. Diversos autores han descrito diferentes requisitos de seguridad (Jefferson 2001, Gerck 2001, Shubina & Smith 2004), de los cuales se puede obtener una visión suficientemente amplia.

En resumen, los requisitos que debe cumplir un sistema de voto electrónico remoto son los siguientes:

- *Legitimidad del votante.* Solo pueden participar votantes autorizados y además se puede aceptar un voto por votante. Tanto en los procesos de elección convencionales como en los que se utilizan sistemas de voto electrónico presencial, este requisito se cumple cuando el participante muestra una identificación que lo acredite como votante autorizado. La autoridad de la elección comprueba la legitimidad del votante verificando que su registro se encuentra en las listas del censo electoral. En el voto electrónico remoto es más complejo realizar dicha autenticación del votante. Comúnmente se han estado utilizando técnicas simples de identificación remota. Por ejemplo, un nombre de usuario y contraseña.

- *Privacidad*. La relación entre votante y voto no debe ser conocida ni deducida. En un proceso de voto convencional se logra ocultar fácilmente la opción elegida por un votante, ya que una vez que este ha sido identificado como legítimo para votar, emite su voto de manera privada y lo deposita en la urna. Esta separación entre voto e identidad del votante es una tarea compleja en el voto electrónico remoto.

- *Precisión*. El resultado de la elección debe proceder exactamente de los votos emitidos de manera legítima, es decir, solo los votos válidos provenientes de votantes legítimos deben ser tenidos en cuenta. Por tanto, los votos duplicados o no válidos deben ser excluidos del escrutinio. Además, debe prevenirse cualquier alteración de los votos. Cualquier intento de quebrantar la integridad de los resultados de la elección debe ser detectado oportunamente.

- *Equidad*. No se deben conocer resultados parciales durante la fase de votación, de lo contrario dicho conocimiento podría influir en la decisión de los votantes que aún no han emitido su voto.

- *Verificación individual*. En un sistema de voto electrónico remoto, cada votante debería poder verificar:

    - que su voto ha sido recibido correctamente por el servidor de votación (verificación de registro correcto) y,

    - que su voto ha sido incluido correctamente en el escrutinio (verificación de escrutinio correcto).

- *Verificación universal*. Un elemento importante para dar fiabilidad a un sistema de voto electrónico remoto es que este sea públicamente verificable, de tal manera que cualquier participante u observador pueda verificar la integridad de los resultados.

- *Incoercibilidad*. Un votante no debería tener la posibilidad de probar a un tercero la opción o candidato que ha elegido en una elección, ya que el poder probarlo facilitaría la coerción o venta de votos.

- *Robustez*. Un sistema de voto electrónico remoto debería ser tolerante a fallos tecnológicos, así como prevenir ataques de denegación de servicio.

 © Oficina Nacional de Procesos Electorales

Por otro lado, un sistema de voto electrónico remoto debería ser resistente a amenazas derivadas de confabulaciones de autoridades deshonestas que intenten llevar a cabo un ataque contra el sistema de votación, por ejemplo, violar la privacidad de los votantes o alterar los resultados de la elección.

Antes de analizar la dificultad que existe para proporcionar la seguridad requerida a los sistemas de voto electrónico remoto es importante notar que incluso los sistemas de voto convencional, es decir, aquellos basados en papeletas de votación, presentan importantes problemas de seguridad. A continuación, se describe algunos ejemplos:

- *Cadena de votos.* Se podría pensar que un ataque de coerción o venta de votos es exclusivo de entornos remotos. Sin embargo, en un sistema de voto convencional se puede presentar un ataque de cadena de votos como el descrito en Jones (2005a). Para llevarlo a cabo, el atacante necesita obtener una papeleta de votación en blanco. Dicha papeleta es marcada con las opciones de voto deseadas por el atacante y la entrega a un votante coaccionado o que desea vender su voto. El votante entra en el recinto de votación ocultando la papeleta. Una vez que un oficial de la elección entrega al votante una papeleta en blanco, el votante accede a la cabina de votación y de manera privada intercambia las papeletas, entonces deposita en la urna la que le fue entregada por el atacante y sale del recinto de votación ocultando la papeleta en blanco. Esta papeleta en blanco será la prueba ante el atacante de que la papeleta depositada en la urna ha sido la encomendada. El atacante tiene entonces una nueva papeleta en blanco, por lo que puede seguir llevando el ataque con el mismo procedimiento tantas veces como personas coaccionadas o vendedoras de su voto tenga disponibles.

- *Prueba del voto.* Además del ataque de coerción descrito en el punto anterior, se puede llevar a cabo un ataque en el que el votante obtenga una prueba de su papeleta marcada. Esto puede lograrse simplemente tomando una fotografía de la papeleta con las opciones marcadas mientras el votante se encuentra en el entorno privado de la cabina de votación. La fotografía es mostrada al atacante para comprobarle que se ha llevado a cabo su petición. Considerando que en la actualidad resulta muy fácil

portar discretamente una cámara fotográfica, por ejemplo, la incluida en la mayoría de los teléfonos móviles, este ataque es fácil de llevar a cabo. Este ataque puede hacerse igualmente en sistemas de voto electrónico presencial, lo que muestra que un ataque de coerción no es exclusivo de los sistemas de voto remoto.

- *Verificación del voto.* En un entorno de voto presencial, el votante deposita su papeleta en la urna física. A partir de ese momento, el votante debe confiar en que su voto será incluido en el escrutinio, ya que no existe la manera de verificarlo. La autoridad de la elección usualmente publica los resultados locales por recinto. Sin embargo, dicha información no le confirma al votante que su voto ha sido contado o que ha sido manipulado antes del escrutinio, o bien que ha sido eliminado o alterado durante los procesos de consolidación de resultados.

¿Por qué es complejo satisfacer los requisitos de seguridad?

El sistema ideal de voto electrónico remoto debería cumplir con todos los requisitos de seguridad descritos en la sección anterior. La mayoría de estos requisitos puede cumplirse mediante la combinación de técnicas criptográficas, políticas y procedimientos. Sin embargo, debido a la naturaleza de un entorno remoto es difícil cumplir algunos de estos requisitos sin debilitar el cumplimiento de otros, como se explica a continuación.

Legitimidad del votante y privacidad

En un contexto de voto electrónico remoto es complicado separar el voto de la identidad del votante, ya que la autenticación del votante y la emisión del voto se llevan a cabo por medio del mismo canal. Para poder sufragar, el ciudadano debe poseer las credenciales de votación que lo acreditarán como votante legítimo, las cuáles son emitidas por una autoridad de la elección. Estas credenciales, que pueden ser, por ejemplo, un nombre de usuario y una contraseña, deben ser validadas al iniciar la sesión de voto. Una vez validadas, se permite que el ciudadano emita su voto. En este punto tenemos entonces un votante autorizado para sufragar y un voto que corresponde a ese ciudadano. Un proceso de autenticación como este pone en riesgo la privacidad del ciudadano, ya que aunque el voto esté cifrado al momento de llegar al servidor de sufragio, se

 © Oficina Nacional de Procesos Electorales

puede conservar la relación del voto con el votante y una vez descifrado aquel, se violaría la privacidad de la persona. Algunos trabajos han abordado este problema, aunque aún existen dificultades para lograr la privacidad del votante de una manera eficiente.

Verificación del voto versus incoercibilidad

El hecho de que un votante pueda verificar que su voto ha sido incluido en el escrutinio podría significar también que es capaz de probarlo a terceras personas. En ese caso, podría facilitarse la coerción o la venta de votos. Se han propuesto esquemas en los que el votante tiene la posibilidad de verificar que su voto se ha contado sin que esto represente que puede probarlo a terceras personas. Ejemplos de estos esquemas los podemos encontrar en Chaum (2004) y Neff & Adler (2003). Dichos esquemas están basados en recibos criptográficos de votación y están enfocados a pautas de sufragio en donde la verificación del voto solo es necesaria en el aspecto de su inclusión en el escrutinio, es decir, en donde se asume que el voto ha sido registrado correctamente, por ejemplo, en los sistemas de voto electrónico presencial. Sin embargo, en entornos remotos de sufragio es imprescindible contar con mecanismos que permitan la verificación del registro correcto del voto. Esto se debe a que los votos son enviados desde una terminal de sufragio que se encuentra fuera del control y supervisión de la autoridad de la elección y mediante una red telemática pública, lo cual podría facilitar la manipulación del voto antes de ser registrado en el servidor de votación. Por su parte, esquemas de voto remoto basados en papeletas precifradas como los descritos en Malkhi (2002) y Storer & Duncan (2005) permiten al votante verificar que su voto se ha registrado correctamente, pero son también propensos a coerción.

Como se ha explicado, existen importantes dificultades para lograr que un sistema de voto electrónico remoto sea seguro y confiable. Generalmente, en una elección hay muchos intereses de por medio. Por esta razón cualquier escenario de votación presenta riesgos de seguridad, debido principalmente a adversarios que tratarán de obtener una ventaja llevando a cabo algún ataque.

Amenazas de seguridad en los sistemas de voto remoto

La mayoría de los requisitos de seguridad en los sistemas de voto electrónico son necesarios en parte debido a las diferentes amenazas que se pueden presentar en dichas plataformas. Las amenazas son eventos inesperados que pueden suponer un peligro a uno o más de los elementos de la elección, por ejemplo, a votos individuales, al resultado de la elección, etcétera. Una amenaza puede ser deliberada o accidental (por ejemplo, a causa de un error o incluso un evento ambiental o natural). Por su parte, un ataque es la realización de una amenaza.

En todo sistema de información existen tres áreas básicas de seguridad que pueden ser afectadas por un ataque: confidencialidad, integridad y disponibilidad. Aplicando estas áreas de seguridad a los sistemas de votación, las principales amenazas son aquellas que podrían llegar a comprometer alguno de los siguientes objetivos:

a) privacidad del votante (confidencialidad),
b) precisión de los resultados (integridad) y
c) continuidad hasta completar el proceso de elección (disponibilidad).

En Morales (2009) se presenta un catálogo genérico de amenazas para los sistemas de voto electrónico remoto. Aun cuando se enfoca específicamente para el escenario de una elección por Internet, puede servir como base para otros sistemas de voto electrónico remoto. Este catálogo se presenta como una guía para comprender cuáles son los principales retos de seguridad que afronta un sistema de voto electrónico remoto. Como afirma Jones (2005b), «un catálogo de amenazas a los sistemas de votación no es una amenaza». El catálogo se describe a continuación:

- *Suplantación de identidad en el proceso de registro.* Si una elección se lleva a cabo de manera remota, es de suponer que para el registro de votantes se utilice también medios remotos. Esto conlleva la posibilidad de que una persona intente suplir la identidad de otra para obtener unas credenciales de votantes válidas.

 © Oficina Nacional de Procesos Electorales

- *Manipulación del censo electoral.* El censo electoral está formado por los datos de los votantes autorizados para participar en la elección. Una manipulación en dicho censo puede causar que un votante legítimo no sea aceptado en la fase de votación. Por otro lado, si se añaden datos de personas ficticias o sin derecho a voto (por ejemplo, debido a la edad) en el censo electoral, se pueden usar esas credenciales que corresponden a datos de votantes no legítimos.

- *Adquirir credenciales de votante.* Antes de la fase de votación, el votante recibe las credenciales de votante que le servirán para autenticarse y votar. Un atacante puede apoderarse de las credenciales de un votante para sufragar en su lugar.

- *Manipulación del software.* El *software* utilizado en cada una de las fases del proceso de elección puede ser un punto de ataque a fin de manipular los procesos que soportan. El *software* puede incluir el sistema de registro, el de configuración de la elección, el de votación, el de consolidación de resultados, etcétera.

- *Daño del hardware o equipo de red.* El *hardware* incluye los terminales de votación, por ejemplo, los servidores, ordenadores personales, etcétera. Por su parte, el equipo de red incluye los elementos que forman los canales de comunicación que se utilizan en los procesos de la elección. Tanto el *hardware* como el equipo de red pueden sufrir daños provocados, accidentales o incluso ambientales. Estos pueden ocasionar que la elección no se lleve a cabo con normalidad o incluso que pueda ser interrumpida.

- *Configuración errónea de la elección.* La configuración de la elección establece los parámetros utilizados para que todos los procesos se efectúen como han sido planeados. Una configuración errónea, que puede ser generada o accidental, puede alterar el funcionamiento de los procesos de la elección, incluso modificar el resultado de esta.

- *Manipulación del voto en la terminal de votación.* En un sistema de sufragio remoto, el ciudadano utiliza un dispositivo personal para emitir su voto. Este podría estar expuesto a ataques que tratan de modificar el voto escogido por el ciudadano.

- *Votar más de una vez.* El proceso de autenticación del votante debe prevenir que un ciudadano sufrague más de una vez en la misma elección. De otro modo, existiría una discrepancia entre la cantidad de votantes que participaron y la de votos recibidos. Esta situación desde luego ocasionaría un resultado de la elección no legítimo. Existen casos en los que el proceso de elección permite rectificar el voto. En dichas situaciones, debe existir un control para que solo el último voto sea tomado en cuenta.

- *Sustitución de votos.* Los votos son recibidos en un servidor y se almacenan en una base de datos. Esta puede ser el blanco de ataques que pretendan sustituir votos a fin de alterar el resultado de la elección. Un control de acceso inadecuado a la base de datos puede dar lugar a este tipo de ataques.

- *Adición de votos ilegítimos.* Al igual que en el ataque anterior, el propósito de la adición de votos es alterar el resultado legítimo de la elección. Esto se puede lograr accediendo a la base de datos en donde se almacenan los votos.

- *Captura de votos.* Debido a que son transmitidos mediante Internet, los votos podrían ser comprometidos por un atacante que logre acceso a la comunicación. Este podría simplemente tratar de conocer el contenido del voto o bien podría actuar como man-in-the-middle[1] para sustituir el voto durante su transmisión.

- *Fuerza bruta para obtener claves privadas de la elección.* La privacidad de los votos radica en gran parte en la fortaleza del algoritmo de cifrado utilizado y en la protección de la clave privada que se utilizará para descifrar los votos. Por esta razón, la clave privada debe permanecer segura durante la elección. Un adversario podría tratar de obtener la clave privada de la elección mediante un ataque de fuerza bruta.[2] Además de la clave privada para descifrar los votos, pueden existir en el sistema de voto

[1] Un ataque de *man-in-the-middle* o ataque de hombre en el medio es aquel en donde el atacante intercepta la comunicación entre dos partes, captura los mensajes provenientes de un punto, los modifica y los reenvía al destinatario, sin que ninguna de las dos partes lo perciba.

[2] Un ataque de fuerza bruta consiste en probar todas las combinaciones posibles de claves hasta obtener la correcta.

 © Oficina Nacional de Procesos Electorales

otras claves privadas susceptibles a un ataque de fuerza bruta. Por ejemplo, las claves utilizadas para firmar digitalmente algunos de los datos.

- *Denegación de servicio.* Evitar que ciertos votantes accedan al sistema de votación puede representar una ventaja para un adversario. Esto se puede dar por medio de un ataque de denegación de servicio (DoS)[3] en el que se inhabilite, por ejemplo, el servidor de registro, el servidor de votación, etcétera.

- *Confabulación de la mesa electoral.* Usualmente, los miembros de la mesa electoral tienen importantes privilegios de manera compartida y generalmente ellos representan diferentes intereses. Sin embargo, una confabulación maliciosa de dichas personas (aun entre algún subconjunto de ellas) puede alterar el resultado de la elección o violar la privacidad de los votantes.

- *Manipulación de los resultados.* Una vez que los votos han sido consolidados y contabilizados, el resultado podría ser manipulado para beneficiar a cierto candidato.

- *Coerción.* En una elección llevada a cabo por medio de un sistema de voto por Internet, tal como en cualquier otro sistema de votación, existe el riesgo de coerción o venta de votos. Un atacante tratará de coaccionar a la mayor cantidad de votantes posible, a fin de obtener una ventaja considerable.

Cada una de las amenazas descritas puede presentarse en una o más fases de la elección.

Vulnerabilidades en un sistema de votación

Un atacante tratará de explotar alguna vulnerabilidad del sistema de votación a fin de comprometer alguno de los objetivos generales de la elección. A continuación, se describe algunos ejemplos de vulnerabilidades que pudieran presentarse en un sistema de voto electrónico remoto mal diseñado:

[3] Un ataque de denegación de servicio consiste en enviar a un servidor una cantidad de solicitudes de conexión (o de algún servicio) mayor a las que puede soportar, de manera que se satura la capacidad de respuesta, lo cual inhabilita a dicho servidor temporalmente.

- *Deficiente sistema de registro de votantes.* El sistema de registro es el medio por el cual se recaba la información de los votantes para formar un censo electoral. Si dicha recolección de datos es ineficiente, no se puede garantizar la correcta verificación de la legitimidad de los votantes durante la fase de votación. Por ejemplo, un votante legítimo podría ser incorrectamente rechazado para votar por un error en la constitución del censo electoral.

- *Deficiente diseño de los mecanismos criptográficos empleados.* Un aspecto esencial en la seguridad de los sistemas de voto electrónico remoto es la criptografía utilizada. Un diseño inapropiado del mecanismo criptográfico podría causar un riesgo importante a la integridad de la elección. El diseño comprende el protocolo, el algoritmo utilizado, la longitud de las claves, el medio de almacenamiento de las claves privadas, etcétera.

- *Proceso de autenticación débil.* Un proceso robusto de autenticación aceptará solo votantes legítimos para emitir un voto. Por el contrario, un esquema de autenticación débil afronta el riesgo de aceptar votantes no legítimos. Por tanto, representa una vulnerabilidad que puede ser aprovechada por un atacante.

- *Control de acceso débil a elementos del sistema de votación.* Los elementos lógicos, como ficheros, bases de datos y claves de cifrado, así como los elementos físicos (servidores, terminales de votación, etcétera), deben ser protegidos de accesos no autorizados. De lo contrario, un atacante podría hacer un uso indebido de estos.

- *Terminales de votación inseguros.* Debido a que en un sistema de voto electrónico remoto las terminales de votación están fuera del control de la autoridad de la elección, existe la posibilidad de que dichas terminales tengan problemas propios de seguridad. Esta es una de las principales vulnerabilidades de un sistema de voto electrónico remoto y podría ser ampliamente aprovechada por un atacante, por ejemplo, insertando algún *software* malicioso que pretenda conocer el contenido del voto o bien modificarlo antes de ser emitido.

- *Canales de comunicación inseguros.* Debido a que algunas de las transacciones llevadas a cabo durante el proceso de elección se llevan a cabo por

 © Oficina Nacional de Procesos Electorales

medio de una red telemática, un canal de comunicación inseguro representa una vulnerabilidad que puede afectar los objetivos de la elección.

- *Sistema de logs deficiente.* Un registro deficiente de las transacciones realizadas durante la elección podría ser un punto de debilidad que no garantiza la detección de manipulaciones en la información. Por tanto, si no se cuenta con un registro eficiente de las transacciones existe una probabilidad mayor de ataques sin detección.

- *Procesos deficientes en la verificación de elementos.* Durante la configuración de una elección se debe efectuar algunos procesos de verificación. Estos procesos tienen el propósito de determinar la correcta configuración y operación de los elementos que participarán en la elección. Por tanto, un proceso de verificación deficiente podría resultar en una situación de vulnerabilidad.

El diseño de un sistema de voto electrónico remoto debe considerar las posibles vulnerabilidades para tratar de evitar que alguno de los objetivos críticos del proceso de elección se vea afectado. Adicionalmente, se debe considerar que en un entorno de votación pueden existir distintos tipos de atacantes, por ejemplo, un votante, un oficial de la elección, un miembro del personal técnico o una persona externa, es decir, aquella que no tiene ningún rol dentro de un proceso de elección.

¿Cómo determinar los riesgos de seguridad?

Un riesgo puede ser definido como la posibilidad de que una vulnerabilidad sea explotada por una amenaza. Aun cuando existen ciertas amenazas y vulnerabilidades propias del voto electrónico remoto que son fácilmente identificadas, los riesgos de seguridad para un sistema de voto electrónico remoto no se pueden generalizar debido a las diferencias en la naturaleza de cada elección. Estas vienen dadas por aspectos organizacionales, jurídicos, sociales y técnicos, los cuales varían de un país a otro e incluso de una elección a otra.

De manera que las amenazas y vulnerabilidades que se describieron previamente pueden servir como base. A partir de allí, se deberá analizar cómo las circunstancias específicas de una elección pudieran presentar nuevas vulnerabilidades. Existen metodologías que permiten realizar un cálculo de riesgos,

dando como resultado una lista priorizada de estos de acuerdo con el impacto y a la probabilidad de ocurrencia.

La tabla 1 resume las amenazas y la forma en que pueden afectar en las diferentes fases de la elección, así como las vulnerabilidades que cada una de esas amenazas puede explotar y que dan como consecuencia un riesgo. Para la implementación de un sistema de voto electrónico remoto se deben considerar estas amenazas y la forma en cómo se pueden llevar a cabo los ataques relacionados, a fin de definir contramedidas que puedan mitigar los riesgos o, al menos, disminuir la posibilidad de que ocurran o de que afecten al proceso de elección.

Amenaza	Objetivo	Fases de la elección	Origen de la amenaza	Vulnerabilidades explotadas
Suplantación de identidad en el proceso de registro	- Integridad - Disponibilidad	- Preparación	- Votante -Oficial - Técnico - Externo	- Deficiente sistema de registro
Manipulación del censo electoral	- Integridad - Disponibilidad	- Preparación - Votación	- Oficial - Técnico - Externo	- Deficiente sistema de registro - Control de acceso débil
Adquirir credenciales del votante	- Integridad - Disponibilidad	- Preparación - Votación	- Votante - Oficial - Técnico - Externo	- Control de acceso débil - Canales de comunicación inseguros - Deficiente sistema de registro
Manipulación del *software*	- Integridad - Confidencialidad - Disponibilidad	- Preparación - Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Procesos deficientes de verificación
Daño del *hardware* y equipo de red	- Disponibilidad	- Preparación - Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Procesos deficientes de verificación
Configuración errónea de la elección	- Integridad - Confidencialidad - Disponibilidad	- Preparación	- Oficial - Técnico - Externo	- Control de acceso débil - Procesos deficientes de verificación
Manipulación del voto en la terminal de votación	- Integridad	- Votación	- Externo	- Deficiente diseño del protocolo criptográfico - Terminal de votación inseguro

 © Oficina Nacional de Procesos Electorales

Votar más de una vez	- Integridad	- Votación	- Votante	- Deficiente sistema de registro - Proceso de autenticación débil
Sustitución de votos	- Integridad	- Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Sistema de *logs* deficiente - Procesos deficientes de verificación
Adición de votos ilegítimos	- Integridad	- Preparación - Votación - Consolidación	- Oficial - Técnico - Externo	- Control de acceso débil - Sistema de *logs* deficiente - Procesos deficientes de verificación
Captura de votos	- Integridad - Confidencialidad	- Votación	- Externo	- Deficiente diseño del protocolo criptográfico - Proceso de autenticación débil - Canal de comunicación inseguro
Fuerza bruta para obtener claves privadas de la elección	- Integridad - Confidencialidad	- Preparación - Votación - Consolidación	- Técnico - Externo	- Deficiente diseño del protocolo criptográfico
Denegación de servicio	- Disponibilidad	- Votación - Consolidación	- Oficial - Técnico - Externo	- Canal de comunicación inseguro
Confabulación de la mesa electoral	- Integridad - Confidencialidad	- Votación - Consolidación	- Oficial	- Deficiente diseño del protocolo criptográfico - Procesos deficientes de verificación
Manipulación de los resultados	- Integridad	- Consolidación	- Oficial - Técnico - Externo	- Deficiente diseño del protocolo criptográfico - Control de acceso débil - Procesos deficientes de verificación - Sistema de *logs* deficiente
Coerción	- Integridad	- Votación	- Oficial - Técnico - Externo	- Proceso de autenticación débil - Canal de comunicación inseguro

Conclusiones

Los sistemas de voto electrónico remoto pretenden solventar algunas necesidades que existen en los sistemas de votación tradicionales e incluso en elecciones en donde se utilizan terminales electrónicas de votación en un ambiente supervisado. El voto postal ha sido desde hace varios años una opción de votación en algunos sistemas electorales en donde se buscó aumentar la participación de los votantes. Sin embargo, dichos sistemas, más allá de las ventajas que ofrecen, presentan serios riesgos de seguridad. Por ello, en diversos países se han explorado e incluso implementado sistemas de voto electrónico remoto. Esto no significa que dichos sistemas sean la solución a todos los problemas de seguridad; de hecho traen consigo nuevos retos por resolver.

En este trabajo se ha presentado un análisis de las amenazas y vulnerabilidades de los sistemas de voto electrónico remoto, y de manera más específica, del voto por Internet. En términos generales, existe una lista larga de riesgos que mitigar. Sin embargo, queda en manos de las autoridades electorales llevar a cabo los procesos adecuados de cálculo de riesgos, a fin de implementar los mecanismos que sean capaces de mitigar y, en algunos casos, eliminar dichos riesgos.

Referencias bibliográficas

Álvarez, R.M., T.E. Hall y B.F. Roberts

2007 *Military Voting and the Law: Procedural and Technological Solutions to the Ballot Transit Problem*. Institute of Public and International Affairs, 16, 1-59.

Chaum, D.

2004 «Secret-Ballot Receipts: True Voter-Verifiable Elections», En: *IEEE Security and Privacy*, vol. 2, N.º 1, pp. 38-47, enero.

ESTONIAN INTERNET VOTING

2005 Disponible electrónicamente en <www.vvk.ee/engindex.html#0003>.

 © Oficina Nacional de Procesos Electorales

Gerck, E.

2001 *Internet Voting Requirements*. The Bell, vol. 1, N.º 7, p. 3, noviembre, 2000, ISSN 1530-048X.

Jefferson, D

2001 *Requirements for Electronic and internet Voting Systems in Public Elections.* In Wote, 2001.

Jones, D

2005a «Chain Voting». Disponible electrónicamente en <http://vote.nist.gov/threats/papers/ChainVoting.pdf>.

2005b *Threats to Voting Systems. A Position Paper. Presented at the Workshop on Developing an Analysis of Threats to Voting Systems*. National Institute of Standards and Technology. Gaithersburg, Maryland. 7 de octubre.

Krimmer, R., M. Volkamer

2005 *Bits or Paper? Comparing Remote Electronic Voting to Postal Voting*. Egov.

Malkhi, D., O. Margo y E. Pavlov

2002 «E-voting without Cryptography» Disponible electrónicamente en <http://citeseer.ist.psu.edu/malkhi02evoting.html> (enero, 2007).

Morales, V.

2009 *Seguridad en los procesos de voto electrónico remoto*. Tesis de doctorado. UPC-Departamento de Telemática.

Neff, A. y J. Adler

2003 *Verifiable e-voting*. Disponible electrónicamente en <www.votehere.net>.

REPUBLIQUE ET CANTON DE GENEVE

2008 *E-Voting*. Disponible electrónicamente en <www.geneve.ch/evoting/english/welcome.asp>.

Storer, T. e I. Duncan

2005 *Two variations of the mCESG pollsterless e-voting scheme*. En: Randal Bilof, *editor, Compsac 05 The 29th Annual International Computer Software & Applications Conference*, pp. 425-430, Edimburgo, julio. IEEE Computer Society.

Shubina, Anna M. y S.W. Smith

2004 «Design and Prototype of a Coercion-Resistant, Voter Verifiable Electronic Voting System», En: *Proceedings of the Second Annual Conference on Privacy, Security and Trust*. University of New Brunswick Fredericton, New Brunswick, Canada, octubre, 2004.

UK PILOT SCHEMES

2007 Disponible electrónicamente en <www.electoralcommission.org.uk/elections/pilotsmay2007.cfm>, mayo.

[Sobre el autor]

Víctor Manuel Morales Rocha

Mexicano. Doctor en Telemática por la Universidad Politécnica de Cataluña. Ha sido gerente de proyectos en eMobile Innovación y Consultoría Móvil. Se ha desempeñado también como investigador en Scytl Secure Electronic Voting. Es actualmente coordinador de la Maestría en Cómputo Aplicado del Instituto de Ingeniería y Tecnología de la Universidad Autónoma de Ciudad Juárez.

 © Oficina Nacional de Procesos Electorales