SISTEMA DE VOTO DEMOCRÁTICO DESDE CUALQUIER ACCESO INTERNET

Pedro Uria Recio, Koldo Espinosa Acereda, Iñaki Goirizelaia Ordorika

Escuela Superior de Ingenieros – Universidad del País Vasco – Alda. Urquijo s/n. 48013 - BILBAO
Dpto. Electrónica y Telecomunicaciones
pedroweb@teleline.es , jtpesacj@bi.ehu.es , jtpgoori@bi.ehu.es

RESUMEN

Abstract: We present a proposal for the design and implementation of a practical, secure and private system for conducting elections over computer networks. The system proposed uses blind signatures to ensure that only registered voters can vote and that each registered voter votes once. Digital signature and encryption are used to maintain votes' privacy and security during the polls. Reliability is achieved by using a redundant protocol and architecture.There are many voting protocols which allow a voter to cast a ballot on his/her own computer but few are designed to maintain the levels of security and privacy that we come to expect from governmental elections in many democratic countries.

1. INTRODUCCIÓN

La razón principal que esgrimen los partidarios del voto vía Internet es que esta nueva tecnología incrementará el nivel de participación, permitirá al electorado estar mejor informado y facilitará el acceso al proceso democrático.

Por el contrario, los detractores del voto por Internet insisten en que la tecnología necesaria para autentificar a los votantes y asegurar la integridad del sistema electoral, o bien no existe aún, o no está lo suficientemente extendida en la sociedad como para ser justa y efectiva.

Todo sistema de voto (electrónico o no) debe cumplir una serie de requisitos que garanticen un buen funcionamiento democrático. Estos requisitos se resumen en las siguientes leyes:

1) El voto es secreto.
2) Cada votante autorizado sólo puede votar una vez.
3) No debe ser posible interferir con el normal funcionamiento del sistema de ningún modo, falsificar la votación ni vender el voto.
4) Todos y cada uno de los votos serán contados con exactitud e incluidos en el resultado final.
5) El sistema debe mantenerse operativo como mínimo durante toda la elección.
6) El sistema debe poder ser comprobado de forma que se detecte cualquier irregularidad.

2. HERRAMIENTAS UTILIZADAS

- **Criptografía:** Se emplea una criptografía de clave pública y privada unida a una o varias claves de clave de sesión aleatoria, tal y como emplean dos protocolos clásicos en el voto por Internet (Sensus [1], Evox [2]). Empleamos criptografía RSA [3].
- **Firma Digital:** La firma digital es el equivalente electrónico a la firma escrita. Esto es, un objeto está unido a un documento asociándolo con el firmante de forma ineludible, única y verificable.
- **Firma Ciega :** Nuestro sistema de voto necesita la utilización de firmas ciegas que permitan a una tercera parte firmar un voto sin poder acceder a él como si se tratase de un sobre con un documento en su interior y un papel de carboncillo. La firma traspasaría el sobre y quedaría reflejada en el documento.
- **Computación Multi-Parte [4]:** Un sistema de computación en el que cada una de las partes que intervienen no pueden acceder a toda la información puede resolverse mediante una parte central de confianza que gobierne el trasiego de información. Un protocolo de computación Multi-Parte sustituye a esta parte central por un protocolo entre las partes. Este es el caso del servidor del sistema de voto en donde quien conozca el voto no puede conocer al votante, ni viceversa.

3. LA AUTENTIFICACIÓN DEL VOTANTE

Los ciudadanos que deseen votar por Internet deberán comunicar su intención a un organismo oficial donde se comprobará su identidad mediante métodos tradicionales. Posteriormente recibirán un CD con sus claves privadas y públicas que les identificarán durante el proceso electoral. El problema que surge es que las autoridades electorales conocen las claves que identifican a cada votante, y esto podría poner en peligro la privacidad del voto. Por ello, el votante genera otro mecanismo de claves con las que ocultará su voto.

4. EL SOFTWARE DEL VOTANTE.

El votante se conecta a una página Web, desde la que se descarga todo el sofware necesario para cubrir el proceso electoral, realizando las tareas de encriptación de los votos y tomando las medidas que SSL ofrece para evitar, en la medida de los posible, ataques causados por hackers como "jamming","man in the middle" o "page jacking". Para evitar estos problemas cada votante emite una cadena de n votos, de los cuales tan sólo uno es válido. El voto válido se puede distinguir de los demás mediante un algoritmo secreto en función de la dirección IP del votante. Los votos no válidos están predefinidos, y si alguno de ellos es modificado se detecta al hacker.

5. EL SISTEMA DE SERVIDORES

El esquema propuesto para el servidor consiste en una serie de entidades destinadas a ser implementadas en diferentes lugares físicos por motivos de seguridad. Estas entidades son:

- N Administradores
- Una matriz de K x L Encargados del Anonimato
- K Contadores

Estas entidades utilizan el protocolo SSL (Secure Socket Layer) [5], así como un un protocolo de computación multi-parte.
El servidor Web va a ser Apache [6] y correrá bajo la plataforma Linux Red Hat. El servidor contiene un cortafuegos que se empleará para evitar inundaciones de demandas por parte de hackers que intenten sabotear las elecciones.

6. EL FUNCIONAMIENTO DEL SISTEMA

El votante llama a una serie de administradores para pedir papeletas de votación. El votante selecciona la papeleta de votación, la compromete, ciega el compromiso, firma el resultado. El votante repetirá este proceso con otras n-1 papeletas cuyo valor es sólo de prueba. Estas n-1 papeletas están prefijadas y son indistinguibles de las papeletas normales. Si un hacker fuera capaz de cambiar el voto antes de ser encriptado podría, sin darse cuenta, cambiar una papeleta de prueba y sería detectado. El votante entrega el compromiso ciego de las n papeletas firmadas (las n-1 de prueba y la válida) al administrador.

Cada administrador consultará su base de datos (mySQL [7]), y si el votante tiene derecho al voto, no ha sido validado previamente por dicho administrador y su firma digital es correcta firmará ciegamente cada voto (los de prueba también), asignará un identificador al votante y devolverá los votos al votante.

Entonces, el votante se dispondrá a repetir el proceso hasta que el voto haya sido firmado por varios administradores. Para que un voto sea tenido en cuenta por cada encargado del anonimato deberá estar firmado digitalmente por la mitad más uno de los administradores. El objetivo de esta redundancia es evitar que un administrador deshonesto envíe votos por gente que no ha votado.

Una vez que el votante ha recibido las firmas necesarias, construirá un mensaje con la lista de n papeletas firmadas por los administradores. Esta lista de votos será encriptada con la clave pública de los contadores (Todos los contadores tienen la misma clave pública). El votante enviará este mensaje a la primera fila de K encargados del anonimato.

Estos K encargados del anonimato comprobarán de forma independiente la firma de los administradores, y almacenará los identificadores que cada uno de ellos han dado al votante para impedir que el votante pueda volver a enviar los mismos votos. Un criterio existente en función de la dirección IP del votante es capaz de separar el voto verdadero de los de prueba. Entonces, los encargados del anonimato almacenan todos los votos válidos encriptados, y cuando acabe la jornada electoral se los pasará en orden aleatorio a la segunda fila de encargados. Estos tienen la misión de impedir la conspiración entre la primera fila de encargados que conocen las direcciones IP de los votantes pero no saben leer sus votos, y los contadores que sí saben leer los votos pero no conocen a los votantes. Para evitar esta conspiración, podrían existir incluso más de dos filas de encargados del anonimato.

Una vez que todos los votos han llegado a los contadores, cada uno de ellos procederá a la decriptación de los votos y recuento paralelamente para evitar la pérdida maliciosa de votos. Si se encuentran discrepancias, el contador que tiene el voto adicional puede probar que existe mostrándoselo al contador que no lo tiene. Las discrepancias podrían resolverse y el recuento sería preciso.

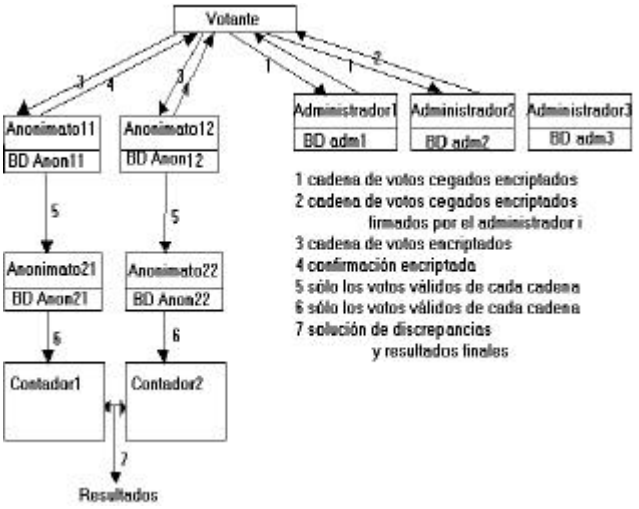

Figura1. Arquitectura del sistema con N=3, K=2 y L=2.

7. CONCLUSIONES

Una vez que los votos son encriptados y firmados se considera imposible que sean descifrados o modificados por partes desautorizadas. No obstante, podrían existir dos posibles agujeros de seguridad en un sistema de setas características:

- En el ordenador del votante podría existir software malicioso que accediese a los votos antes de ser encriptados. Para evitar esto se plantea la utilización de cadenas de votos o formatos de papeletas variables.
- En el sistema de servidores podrían exitir conspiraciones entre las entidades que lo componen. Esto se dificulta mediante una arquitectura redundante de entidades distribuidas.

8. REFERENCIAS

[1] SENSUS: http://www.ccrc.wustl.edu/~lorracks/sensus/
[2] EVOX: http://theory.lcs.mit.edu/~cis/voting/voting.html
[3] RSA: http://www.rsasecurity.com/
[4] Secure multy-party computation http://www.wisdom.weizmann.ac.il/~oded/pp.html
[5] Open SSL: http://openssl.org
[6] The Apache Software Foundation: http://www.apache.org
[7] my SQL: http://www.mysql.org
[8] Securepoll: http://www.securepoll.com
[9] California Internet Task Voting Force: http://www.ss.ca.gov/executive/ivote/
[10] Forschungsgruppe Internetwahlen, Universität Osnabrück: http://www.i-vote.de/index.html