UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Análisis teórico de la seguridad en el sistema de votación electrónica Evotebox

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática

Autor: Joaquim Molina López
Tutor: Diego Alvarez Sanchez

Curso 2018-2019

Resum

Aquest projecte tracta de realitzar un estudi de les vulnerabilitats que afecten el sistema de votació electrònica Evotebox, desenvolupat per la Càtedra de Govern Obert de la UPV per a la votació dels pressupostos participatius de l'Ajuntament de València DecidimVLC.

Així mateix es detalla el disseny del sistema Evotebox i quines són les tecnologies utilitzades al projecte, considerant que conèixer com s'ha dissenyat un sistema és necessari per conèixer les vulnerabilitats que afecten aquest.

A més, es realitza un estudi sobre algunes implementacions de diferents tipus de votacions electròniques en el món i es detallen quins són els requisits de seguretat necessaris per a aquest tipus de sistemes de manera que pugui oferir les mateixes garanties que les votacions tradicionals.

Paraules clau: Evotebox, vulnerabilitats, seguritat, Raspberry, NFC, vot electrónic

Resumen

Este proyecto trata de realizar un estudio de las vulnerabilidades que afectan al sistema de votación electrónica Evotebox, desarrollado por la Cátedra de Govern Obert de la UPV para la votación de los presupuestos participativos del Ayuntamiento de Valencia DecidimVLC.

Así mismo se detalla el diseño del sistema Evotebox y cuales son las tecnologías utilizadas en el proyecto, considerando que conocer como se ha diseñado un sistema es necesario para conocer las vulnerabilidades que afectan al mismo.

Además, se realiza un estudio sobre algunas implementaciones de diferentes tipos de votaciones electrónicas en el mundo y se detallan cuales son los requisitos de seguridad necesarios para este tipo de sistemas de forma que pueda ofrecer las mismas garantías que las votaciones tradicionales.

Palabras clave: Evotebox, vulnerabilidades, seguridad, Raspberry, NFC, voto electrónico

Abstract

This project tries to carry out a study of the vulnerabilities that affect the electronic voting system Evotebox, developed by the "Cátedra de Govern Obert" of the UPV for voting on the participatory budgets of the Valencia city council DecidimVLC.

Likewise, the design of the Evotebox system is detailed and the technologies used in the project, considering that knowing how a system has been designed is necessary to know the vulnerabilities that affect it.

In addition, a study is made on some implementations of different types of electronic voting in the world and details what are the security requirements necessary for this type of systems so that it can offer the same guarantees as traditional voting.

Key words: Evotebox, vulnerabilities, security, Raspberry, NFC, electronic voting

Índice general

Índice de figuras

CAPÍTULO 1
Introducción

Las tecnologías de la información y comunicación llevan poco tiempo formando parte de nuestras vidas. Sin embargo, ha provocado muchos avances en todos los ámbitos de la vida como la forma de relacionarnos, una nueva revolución industrial mejorando los tiempos y costes de fabricación, e incluso ha cambiado la cultura en nuestra sociedad.

La política también se ha adaptado a este cambio, el uso de las redes sociales (Youtube, Instagram, Facebook) o los portales de noticias en internet son herramientas habituales para difundir sus mensajes y llegar a la ciudadanía sin necesidad de acudir a los medios de comunicación convencionales como la televisión o la radio.

No solo ha cambiado la forma en la que se realiza política, también ha cambiado la forma en la que se desarrolla la democracia, a través de portales de transparencia y consultas a la ciudadanía se puede participar en las decisiones que se toman en los gobiernos, permitiendo una participación directa de la ciudadanía y ejerciendo una presión y control sobre los gobiernos.

Como ejemplo, el ayuntamiento de Valencia puso en marcha la consulta ciudadana DecidimVLC sobre los Presupuestos Participativos de Inversiones, donde la ciudadania pudo implicarse y participar en la toma de decisiones sobre parte del presupuesto municipal destinado a realizar inversiones.

Figura 1.1: Cartel de DecidimVLC 2018-209

Estos nuevos proyectos plantean nuevas mejoras en el sistema de votación, permitiendo la entrada de el voto electrónico o urna digital como solución, gracias a la reducción de costes y una mayor facilidad en el recuento de votos.

Según Yrivarren Lazo [1] el voto electrónico es "un sistema de sufragio que utiliza una combinación de procedimientos, con componentes de hardware, software y red de comunicaciones que permiten automatizar los procesos de identificación del elector, de emisión de votos, de conteo de votos, de emisión de reportes y de presentación de los resultados, de un proceso electoral, referendo y otras consultas populares". Este nuevo sistema de votación que ofrece la tecnología puede representar un gran avance en el desarrollo de las votaciones y una solución al problema de participación electoral que sufre la Unión Europea en las elecciones y en los referéndum [1].

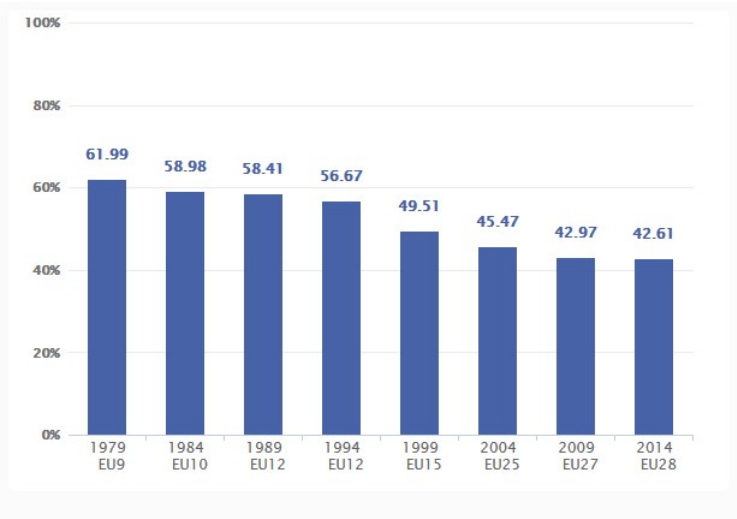

Figura 1.2: Participación electoral en Europa desde 1979

El voto electrónico permite que los electores tengan una mayor facilidad al ejercer su derecho al voto y además de cara a la administración también se reduciría el gasto a largo plazo para desarrollar una votación y permitiría conocer los resultados del escrutinio de los votos de manera fiable y más rápida.

1.1 El voto electrónico

El voto electrónico se utiliza en una gran cantidad de paises, desde India hasta Argentina se ha utilizado este sistema para mejorar en diversos aspectos de su proceso electoral. En la actualidad el voto electrónico puede servir para el desarrollo de la democracia, generando confianza en la gestión electoral o aumentando la eficiencia del proceso electoral en general[4].

Con una correcta implementación, el voto electrónico puede convertirse en una herramienta para perseguir el fraude electoral, acelerar el procesamiento de los resultados, ampliar la accesibilidad y en definitiva conseguir que sea más cómodo para la ciudadania. Aunque no todos los proyectos realizados han conseguido cumplir con todos los requisitos necesarios para generar esa confianza, debido a que la tecnología no está exenta de problemas.

Existen dos tipos diferentes de votaciones electrónicas, el primero seria el voto electrónico remoto, también conocido como voto por internet, es el sufragio donde el voto se transmite a través de la red con un dispositivo. Permite al elector votar desde cualquier lugar facilitando el ejercicio del derecho de sufragio.

[1] http://www.europarl.europa.eu/pdf/elections_results/review.pdf

En cambio, la votación por internet plantea graves problemas para la integridad de la votación, debido a que es complicado garantizar que el voto lo emite realmente el elector o que no ha sido manipulado.

El segundo tipo de votación es el voto electrónico presencial, es el sufragio que se ejerce en el colegio electoral a través de un sistema electrónico. Así mismo, en este apartado se pueden definir tres casos:

- Voto electrónico de forma opcional, complementando el voto en papel tradicional.
- Voto electrónico de forma complementaria, a diferencia de la anterior el uso del sistema electrónico seria necesario para la votación.
- Voto electrónico basando únicamente en el uso del sistema electrónico.

1.2 ¿Qué es Evotebox?

Evotebox es un sistema de votación electrónica presencial utilizado para la consulta DecidimVLC del Ajuntament de València, es uno de los proyectos que se han desarrollado dentro del marco de las políticas de participación para aumentar la implicación de la ciudadanía. Ya que en las anteriores ediciones, la votación se realizó a través de internet en la página web o con algunos puntos de votación habilitados por el gobierno municipal, en las últimas votaciones se dispuso de urnas digitales para realizar el voto electrónico presencial.

Está desarrollado con tecnologías libres y abiertas, creando herramientas de participación útiles y de calidad que puedan aportar una solución e influir en los aspectos que afectan a la vida de los ciudadanos.[2] [3]

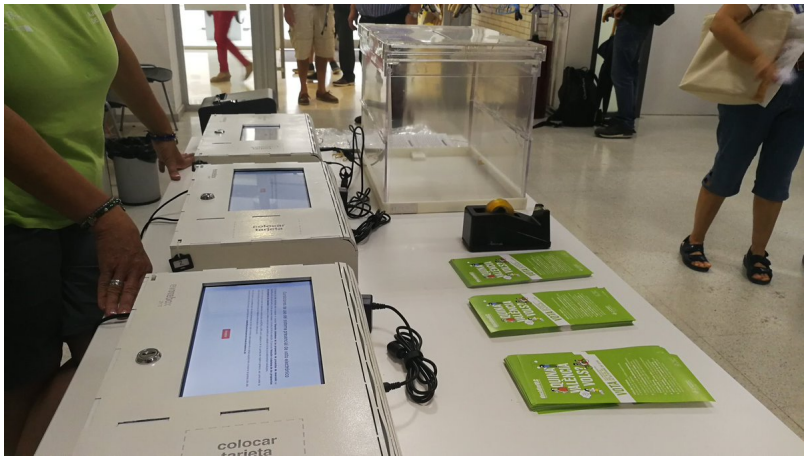

Figura 1.3: Votación DecidimVLC con Evotebox

[2] https://www.inf.upv.es/www/etsinf/es/la-catedra-govern-obert-impulsa-el-desarrollo-de-un-sistema-presencial-de-votacion-electronica/

[3] https://twitter.com/diegoalsan/status/1044537926279933954

1.3 Motivación

El componente principal de la democracia es, que el pueblo tiene que tener poder dentro de la organización social, y para poder ejercerlo en la sociedad actual se utilizan las votaciones como forma de tomar decisiones que más se ajusta a esa idea principal. Por ello creo que, junto al avance en el uso de las nuevas tecnologías, el sufragio activo se debe adaptar a los nuevos tiempos utilizando la votación electrónica como un instrumento más.

En Valencia se ha utilizado por primera vez las urnas digitales o votación electrónica para facilitar la votación física de las propuestas de DecidimVLC [4], además esta tecnología ha sido desarrollada por la Cátedra de Gobierno Abierto de la UPV. Tuve la suerte de apoyar en el desarrollo y el diseño del sistema con el Àrea Hackers Cívics, por lo que este trabajo se puede dejar como documentación del proyecto y así poder aprovechar en un futuro el trabajo hecho para mejorar el diseño y conseguir una mejor solución al problema.

Asimismo, en este proyecto se utilizan diferentes tecnologías de software y hardware por lo que he tenido de aprender tanto en alto nivel como a bajo nivel el funcionamiento de las tecnologías implicadas, conociendo las principales vulnerabilidades asociadas a estas tecnologías aumentando mis conocimientos en el mundo de la ciberseguridad.

1.4 Objetivos

Los objetivos por cumplir en el estudio son los siguientes:

- Comprender las tecnologías utilizadas en el desarrollo de Evotebox.
- Realizar un pequeño estudio de los diferentes sistemas de votación electrónicos que existen. Conocer donde se han implementado y se utilizan los sistemas de votación electrónicos.
- Analizar los puntos por los que un sistema de votación electrónica es confiable y se puede implementar en la sociedad.
- Comprender las vulnerabilidades asociadas al diseño y a las tecnologías utilizadas en el sistema Evotebox.
- Explicar como un sistema de votación electrónico puede llegar a ser confiable y utilizado en diferentes tipos de votaciones.

[4] https://decidimvlc.valencia.es/

1.5 Estructura de la memória

Este trabajo de fin de grado tiene un total de ocho capítulos. A continuación, se detallan brevemente el contenido de los capítulos a partir de la introducción.

- Capítulo 2: Estado del Arte, presenta el estado de la seguridad en los sistemas de votación electrónicos y algunos ejemplos realizados en Europa y América, haciendo énfasis en los problemas de seguridad que se han descubierto.
- Capítulo 3: Análisis del problema, cuenta con tres secciones, primero se realiza un análisis de las características de seguridad que son necesarias en los sistemas de votación electrónica, en la segunda se introducen las tecnologías de seguridaden el ámbito del voto electrónico y finalmente se analiza el marco legal al que están sometidas las votaciones electrónicas en España.
- Capitulo 4: Diseño de la solución, se describe el funcionamiento y el diseño de Evotebox con hincapié en el hardware y software utilizado. Además se detallan las tecnologías utilizadas en Evotebox.
- Capítulo 5: Análisis de las vulnerabilidades, se realiza un análisis de las vulnerabilidades que afectan al sistema Evotebox tanto a escala de hardware o físico como a escala de software.
- Capítulo 6: Propuesta de soluciones, se detallan algunas soluciones propuestas para las vulnerabilidades analizadas en el capítulo anterior.
- Capítulo 7: Conclusiones, se presentan las diferentes conclusiones obtenidas al largo del trabajo.

CAPÍTULO 2
Estado del arte

Actualmente, son muchos los países en los que se han realizado estudios o pruebas para implantar la votación electrónica [1]. En la siguiente imagen se muestran todos los países que actualmente está totalmente implantado el proceso, existe un estudio o implantación parcial o se encuentra legalmente prohibido o paralizado.

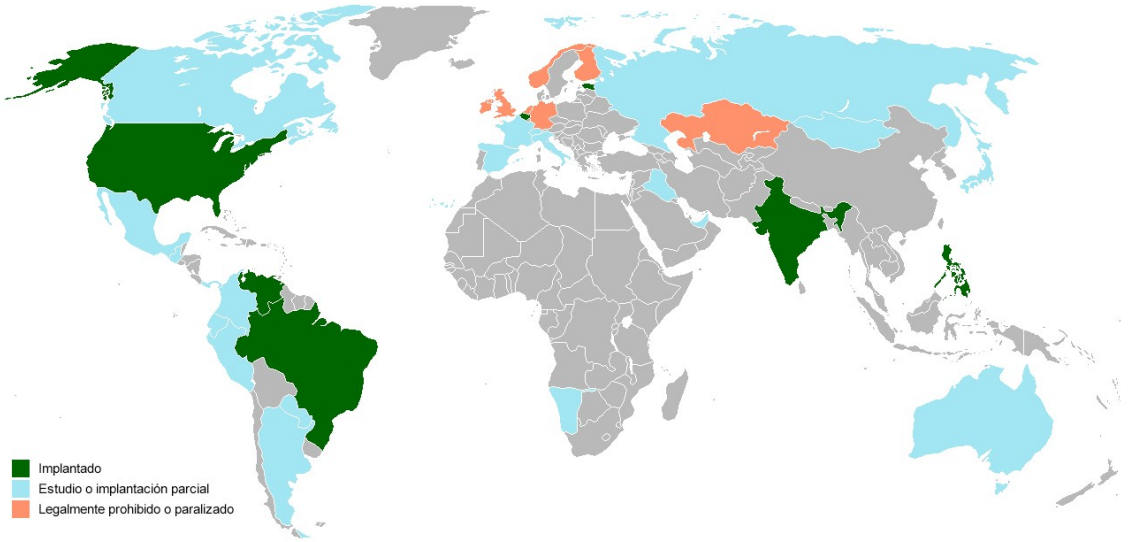

Figura 2.1: Voto electrónico en el mundo.

Como se puede observar existen una gran multitud donde se ha implantado la votación electrónica, entre ellos Estados Unidos o Brasil. España se encuentra en los países que se ha estudiado su implantación y también dentro de la Unión Europea se encuentran países donde se ha prohibido legalmente su implantación como Alemania o Inglaterra.

En esta sección se analizan las diferentes alternativas de votación electrónica que se han implementado en países como Estados Unidos, Argentina u Holanda. Este análisis pretende mostrar las dificultades y las vulnerabilidades que se han podido encontrar en el uso de los sistemas de votación electrónica en diferentes procesos electorales.

[1] http://www.euskadi.eus/informacion/voto-electronico-voto-electronico-en-el-mundo/web01-a2haukon/es/

2.1 Seguridad en los sistemas de votación electrónicos

Existen diferentes características de seguridad necesarias en todos los procesos que engloba una votación electrónica, en este sentido se han realizado diferentes estudios generando una serie de especificaciones y requerimientos con los que los sistemas de votación electrónica se pueden probar para determinar si cumplen el estándar.

En Europa existe la recomendación[18] del Comité de Ministros del Consejo de Europa a los Estados Miembros, donde se especifícan los aspectos legales, procedimentales y técnicos para que la votación electrónica pueda desarrollarse correctamente.

Este documento no entra dentro de los aspectos más técnicos, en cambio se centra en detallar los requisitos mínimos que son necesarios en estos procedimientos, como la accesibilidad, interoperatividad, seguridad, etc. Todos los Estados Miembros de la Unión Europea si desean llevar a cabo una votación electrónica deben de asegurarse cumplir cada uno de los aspectos detallados en el documento.

A continuación, se detallan los puntos principales técnicos del documento:

- Accesibilidad: Se adoptarán medidas para garantizar el acceso a los servicios que se utilicen, también se dispondrán de medios adicionales si lo requiere el usuario.
- Interoperabilidad: Se utilizarán estándares abiertos para garantizar la interoperativilidad entre los componentes, el estándar recomendado es el Election Mark-up Language (EML).
- Sistemas operativos: Se publicará el listado de software utilizado en las elecciones o referéndums electrónicos. Además, se habilitará los mecanismos de backup en caso de que surja algún problema. Los equipos deben de ser revisados y deberán de ubicarse en un lugar seguro.
- Seguridad: En este apartado realiza 4 distinciones:
    1. Requisitos generales: Se adoptarán medidas técnicas para que en caso de fallo no sea posible la pérdida de datos, también el sstema debe de proteger los datos almacenados para garantizar que protege la privacidad y su autenticidad.
    2. Requisitos en las etapas previas a la emisión del voto: La autenticidad, disponibilidad e integridd de las listas de Censo Electoral y de las candidaturs ha de ser mantenida y además también debe de ser verificable el registro de los votantes.
    3. Requisitos en el momento de la emisión del voto: se salvaguardará la integridad de los datos transmitidos provenientedes de la etapa previa de la emisión del voto, una vez terminado el periodo de votación, ningún elector esta autorizado para entrar al sistema.
    4. Requisitos en las etapas posteriores a la emisión del voto: en el proceso de conteo de votos emitidos, se contarán de manera exacta y podrá ser reproducido. Finalmente se mantedra la disponibilidad y el resultado del escrutinio durante el tiempo que se estime oportuno.
- Auditoría: en este partado también se divide en 4 etapas:
    1. Generalidades: Se diseñará un sistema de auditoría como parte integrante del sistema de votación.
    2. Grabación: El sistema ha de grabar tiempos eventos y acciones, como por ejemplo los ataques infringidos al sistema, los fallos o mal funcionamiento del sistema y otros eventos que hubieran puesto en peligro el sistema.

3. Seguimiento: Permitirá supervisar las elecciones y verificar que los resultados respetan las previsiones legales en vigor.
4. Verificación: El sistema permitirá comprobar que las elecciones han cumplido la normativa en vigor, con el fin de verificar que los resultados reflejan de manera exacta el número de votos emitidos.
5. Otros: El sistema debe de estar protegido contra los ataques que puedan corromper, alterar o generar la perdida de los registros hehcos por el sistema de auditoría.

- Certificación: Los estados miembros son los encargados de iniciar el proceso de certificación que permita que cualquier componente electrónico pueda ser puesto a prueba para lograr el certificado de cumplimiento de los requisitos técnicos descritos en la recomendación del Comite de Ministros del consejo de Europa.

En Estados Unidos existe el Voluntary Voting System Guidelines (VVSG)[3] que son un conjunto de especificaciones basados en la funcionalidad, accesibilidad y la seguridad. La organización Help America Vote Act (HAVA)[2] encarga a la organización EAC[3] mantener y desarrollar el documento. Del mismo modo que el documento desarrollado por la Comisión de Ministros del Consejo de Europa el documento VVSG marca los requisitos de seguridad mínimos pero no detalla sobre las tecnologías a utilizar.

Además de estos dos documentos existen más estudios realizados como el .Análisis de factibilidad en la implementación de tecnología en diferentes aspectos y etapas del proceso electoral"[7], realizado por el Consejo Nacional de Investigaciones Científicas y Técnicas de Argentina, pero al igual que en los dos documentos anteriores no se detallan en las tecnologías a utilizar, sino que realiza un estudio de los requerimientos necesarios en el proceso de votación electrónica.

Gracias a estos estandares y estudios, se han realizado la creación de distintas implementaciones de votaciones electrónicas. A pesar de ello, las auditorias realizadas no son públicas y no se puede realizar un estudio detallado del estado de las vulnerabilidades que existen en este tipo de sistemas.

Referente al sistema de votación electrónica de Estados Unidos existe un documento del 2007 retirado de la página web oficial[4] pero que aún se mantiene por la organización independiente Verified Voting[5]. Este análisis se centra en el sistema de votación Diebold (AccuVote-TSX DRE, AccuVote-OS, escanner óptico y el sistema de gestión de la elección GEMS) y realiza una auditoría del código fuente.

Las principales vulnerabilidades encontradas son resumidas en cuatro categorias principales:

1. Software malicioso: un atacante puede instalar software malicioso en el sistema de votación o el sistema de gestión de la votación, alterando la elección y los resultados.

2. Susceptible a virus: un virus puede permitir al atacante que solo tiene acceso a unas pocas máquinas propagarse a través de la red, en un ataca a gran escala no seria necesario el acceso físico a todas las máquinas.

[2]https://www.eac.gov/about/help-america-vote-act/
[3]https://www.eac.gov
[4]https://www.sos.ca.gov/voting-systems/oversight/ttbr/diebold-source-public-jul29.pdf
[5]https://www.verifiedvoting.org/about-vvo/

3. Fallos al proteger el secreto del voto: AccuVote-TSX DRE registra los votos con el tiempo de voto de cada emisión, permitiendo a los trabajadores de la elección a obtener el registro del tiempo y descubrir quien ha votado observando la votación.

4. Fallos de control: el sistema Diebold falla al realizar el control de los trabajadores de la votación con acceso al sistema de gestión GEMS para que no se excedan en sus permisos. Cualquiera cona acceso al servidor GEMS puede modificar los votos o instalar malware para comprometer a las máquinas de votación.

Diferentes investigadores han realizado auditorias independientes en los años siguientes para AVS WinVote [6], AccuVote TS &TSx[7] y iVotronic [8] en todas estas auditorias el principal problema es el fácil acceso a los componentes hardware para poder manipularlos, permitiendo modificar el sistema o implantar algún software malicioso cambiando las tarjetas de memoria.

2.2 Casos reales

2.2.1. Estados Unidos

En 1892 se utilizo la primera máquina de votación denominada "Myers Automatic Booth", un sistema basado en palancas mecánicas donde a cada candidato se le asignaba una palanca. A partir de 1930 se instalaron en las principales ciudades de Estados Unidos y en 1960 casi la mitad de la población votaba con estas máquinas.

A partir de 1980 han existido cinco sistemas de votación diferentes, máquinas de palanca, tarjetas perforadas, papeletas de votación con o sin sistemas de escaneo óptico y máquinas de grabación electrónica directa o DRE (máquinas que graban los votos por medio de una papeleta de votación a través de una pantalla con botones o digitales).

Poco a poco se empezó a incorporar en las siguientes elecciones diferentes tecnologías para la realización de la votación e incluso en las elecciones presidenciales del 2000 los militares destinados fuera del país votaron a través de internet. En estas últimas elecciones se detectaron algunas incidencias de las tarjetas perforadas en el proceso de recuento de votos.

En 2002 se aprueba la ley federal Help America Vote Act, que establece un organismo de control Election Assistance Commissión (EAC) para delinear recomendaciones y guías para los sistemas de votación. El primer documento Voluntary Voting System Guidelines se elaboró en abril del 2005 aunque posteriormente se modifico para incluir los diferentes aspectos de seguridad y establecer estándares y métodos de prueba para los sistemas de votación electrónica.

Además, esta organización lleva a cabo un registro con todos los problemas asociados sobre los dispositivos que se usan en las elecciones (Voting System Reports Collection[5], 2017), el último fallo reportado se trata del descubrimiento en Def Con de Las Vegas, una de las conferencias de hacking más famosas, de vulnerabilidades en la infraestructura y en siete de los modelos utilizados a lo largo de EE.UU.

Fueron distintos los dispositivos a los cuales se les encontró vulnerabilidades[6], en la máquina Diebold ExpressPoll-5000 se encontraron usuarios y contraseñas no robustas y almacenadas sin cifrar como 'password' o la contraseña de administrador 'pasta' también

[6]https://freedom-to-tinker.com/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/
[7]https://www.verifiedvoting.org/resources/voting-equipment/premier-diebold/accuvote-tsx/
[8]https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/

Figura 2.2: Diebold Election Systems

en la máquina Dominion AVC Edge descubrieron que no existia ninguna comprobación en la tarjeta de arranque y se podía modificar por otra tarjeta de arranque controlada por el atacante.

2.2.2. Argentina

El 2003 la provincia de Buenos Aires fue pionera con la Ley 13.082 que facultaba la implantación de sistemas de voto electrónico en los distritos, se eligió el sistema de votación DRE con el uso de papeletas electrónicas y transmite datos de votación a través de una red pública.

Desde el 2009 se utiliza en la provincia de Salta, Argentina, el sistema de Boleta Única Electrónica, "Vot.Ar" y fue implementado para las elecciones a Jefe de Gobierno del 2015. El sistema fue diseñado por empresas privadas y ONGs en conjunto con el Tribunal Electoral de Salta y se ha llegado a utilizar hasta en ocho elecciones en la provincia.

El sistema "Vot.Ar" utilizaba una conexión a Internet para el envió del recuento de votos que se realizaba en cada mesa a un servidor principal donde la autoridad electoral tomará los datos para el escrutinio provisional.

Los investigadores descubrieron una vulnerabilidad [9] que residía en el uso de los certificados SSL para la verificación del envío de los datos a través de la red, cada técnico en cada uno de los centros de votación tenía que descargar los certificados correctos a través de una URL:

https://caba.operaciones.com.ar/media/certificados/CABA_<COMUNA>_<NUMERO>-<NOMBRE CENTRO>.tar.gz

Debido a que los 791 centros de votación se habían publicado días antes se podía modificar la URL para descargar todos los certificados de los diferentes centros, además el nombre de usuario del sistema en el centro se trataba del apellido seguido del nombre

[9] https://github.com/HacKanCuBa/informe-votar

Figura 2.3: Máquina de votación de Vot.ar

del técnico y la contraseña su dirección de correo electrónico, así lo detallan los manuales distribuidos por la organización[10].

2.2.3. Holanda

Ha sido pionero en la utilización del voto electrónico, en 1965 se aprobó el uso de máquinas para la emisión del voto y a partir de la década del 90 se promovió la adopción de equipamiento DRE. A pesar de ello debido a los crecientes problemas de confianza sobre las garantías de los sistemas de votación electrónica en mayo de 2008 se decidió retomar el voto en papel con recuento manual.

Los principales problemas que detectaron fueron dos:

- Falta de verificalidad y código cerrado: el código estaba protegido por derechos a la propiedad del proveedor y los resultados de las auditorias eran secretos. Por tanto, existía una imposibilidad de acceder al sistema para evaluarlo.
- Vulnerabilidades al sistema: el Servicio de inteligencia Holandés demostró que se podía "escuchar" los votos desde una distancia de 40 metros usando un dispositivo Van Eck phreaking[11], donde a través de emisiones electromagnéticas se puede espiar el contenido de un monitor LCD y CRT.

Además, diversos grupos de investigadores demostraron algunos ataques permitiendo modificar el recuento o que la máquina ejecute otro código distinto al original. Debido a estos motivos Holanda paralizó las implementaciones del voto electrónico volviendo a las votaciones de papel original.

[10] https://github.com/prometheus-ar/vot.ar/blob/master/docs/informacion-de-interes.pdf
[11] https://es.wikipedia.org/wiki/Interferencia_de_Van_Eck

2.3 Crítica del estado del arte

Como se ha observado estas tres implementaciones de la votación electrónica no han sido exitosas, llegando incluso a abandonar el uso de las urnas digitales, debido al miedo de que las urnas sean manipuladas por atacantes y la votación sea suspendida, como fue el caso de Holanda.

Sin embargo la mayor parte de las vulnerabilidades existentes en los sistemas de votación electrónicos son, fallos en sus implementaciones o desarrollos cerrados donde no se han seguido las recomendaciones dadas por los organismos internacionales y además, no se ha auditado correctamente el sistema.

Debido a ello, es necesario que en el desarrollo de este tipo de soluciones existan estudios y metodologías seguras para poder realizar un correcto desarrollo además son necesarias las auditorias por investigadores externos que certifiquen su funcionamiento.

Estudios como los antes mencionados del Comite de Ministros del Consejo de Europa o de la EAC de Estados Unidos permiten tener una base para el desarrollo de estos sistemas, a pesar de ello, no se siguen complementamente las recomendaciones y en consecuencia las votaciones realizadas no consiguen generar confianza en la ciudadanía.

Estos estudios deben ser impulsados por los gobiernos o por las asociaciones internacionales y auditar que se siguen los estándares recomendados, de esta forma se podrá llevar a cabo un avance tecnológico en los procesos de sufragio actuales para poder utilizar los sistemas de votación electrónicos.

CAPÍTULO 3
Análisis del problema

Una vez detallados algunas de las implementaciones realizadas en el apartado anterior, se analizan los diferentes aspectos de seguridad que deben de cumplir los sistemas de votación electrónica y el marco legal en España.

3.1 Análisis de la seguridad

Las votaciones electrónicas deben de cumplir las mismas garantías que el voto tradicional, el voto ha de ser libre, secreto y seguro.

Según el informe[7] del Consejo nacional de investigaciones científicas y técnicas son necesarios los siguientes requisitos para el correcto desarrollo del sistema de votación:

- Usabilidad: que sea sencillo para el usuario la utilización del sistema de votación electrónico al realizar cierta tarea.
- Seguridad: capacidad del sistema para proteger los datos y la información de accesos no autorizados o alteración de los datos. En definitiva, debe de atender a las propiedades ACID (accesibilidad, confidencialidad, integridad, disponibilidad).
- Auditabilidad: el sistema debe de ser capaz de ofrecer la información necesaria para poder realizar una auditoría, tanto a escala de software como de hardware.
- Verificabilidad: habilidad para demostrar que un sistema ha sido construido y se comporta de acuerdo con sus especificaciones.
- Desempeño: capacidad del sistema para cumplir eficazmente con sus especificaciones.
- Escalabilidad: posibilidad de despliegue y operación del sistema con mayores costes computacionales y mayor crecimiento que le permita funcionar eficientemente.
- Confiabilidad: capacidad del sistema para evitar estados o condiciones que puedan causar problemas o daños, es deseable que se pueda restablecer a ciertos estados de recuperación.
- Robustez: capacidad del sistema de tener alternativas para cumplir con el resultado, por ejemplo, la incorporación de redundancia con modos de fallo independientes para que si el sistema principal falla, el secundario o terciario pueda suplantarlo.

Algunos de estos atributos se pueden poner en contraposición unos con otros, dependiendo de los requerimientos que se desean implementar en cada votación, como por ejemplo: desempeño versus seguridad o seguridad versus usabilidad.

Estos requisitos se pueden tomar como referencia a la hora de realizar un desarrollo de un sistema de votación ya que se adaptan correctamente a las garantias que tiene el voto tradicional.

3.2 Tecnologías de seguridad en el ámbito del voto electrónico

En cada uno de los países donde se han implantado los sistemas de voto electrónico se ha desarrollado de forma diferente y por tanto cada implementación presenta tecnologías de seguridad diferentes dependiendo de los requisitos de la votación.

En las votaciones por internet se produce el voto a través del uso de las redes, en estas implementaciones se suelen utilizar diferentes capas para mantener los requisitos mencionados en el apartado anterior[1].

- Cifrado de punto a punto: el voto se genera y transmite cifrado, además se utiliza un esquema de descifrado para asegurar la anonimidad del voto.
- Firmado digital: se utiliza un firmado digital para asegurar la integridad del voto.
- Corrección de voto: los servidores comprueban que el voto recibido es válido, en caso contrario se descarta el voto.

Los sistemas de votación electrónica también pueden realizarse físicamente en los centros de votación, estos sistemas son comúnmente utilizados en EEUU, donde existen unas guías de seguridad para el correcto funcionamiento de la votación. [2]

Uno de los principales retos se centra en el desarrollo de hardware seguro, ya que en la mayoría de las aplicaciones si existe un hardware inseguro provocara que el software se vea comprometido. Por ello las principales contra medidas en la seguridad hardware de las máquinas de votación físicas son:

- Módulo de seguridad hardware, es un dispositivo criptográfico basado en hardware que permite la generación de claves criptográficas seguras.
- Cifrado de los datos almacenados.
- Barreras físicas para evitar el acceso a los componentes físicos.

Además, si el voto almacenado se transmite a través de la red pero mediante el uso de un sistema físico en un colegio electoral, se necesitan las medidas de seguridad para las votaciones a través de internet.

3.3 Análisis del marco legal en España

Los procesos electorales se encuentran regulados en la Ley Orgánica 5/1985 [10], de 19 de junio, de Régimen Electoral General (LOREG) y por su desarrollo por el Real Decreto 605/1999, de 16 de abril, de regulación complementaria de los procesos electorales, modificado por el Real Decreto 1382/2002, de 20 de diciembre.

[1] https://www.scytl.com/en/online-voting-technology-security/
[2] https://www.eac.gov/election-officials/election-security-preparedness/

En el primer capítulo se detallan los principales aspectos del derecho a voto como el voto a mayores de edad, inscritos en el censo o la posibilidad de votar por correo, entre otros. También las papeletas y sobres electorales están reglamentados en los artículos 70 y 71 de la LOREG [3], se establece que las Juntas Electorales competentes aprobarán el modelo oficial de las papeletas. Además, en el artículo 4 del RD 605/1999 concreta que las papeletas electorales se confeccionaran en papel en blanco y la impresión se realizará por una sola cara. En todo momento se refiere a la votación impresa y no hay ninguna mención al voto electrónico.

En la Ley Orgánica 2/1980, de 18 de enero, sobre la regulación de las distintas modalidades de referéndum tampoco se prevé la posibilidad de la utilización del voto electrónico.

En ninguna de las modificaciones de la legislación electoral se ha introducido la posibilidad del voto electrónico, para poder implantarlo en España seria necesaria una reforma legislativa para incluir todos los aspectos de las votaciones electrónicas.

En cambio, en relación con las actas de constitución, sesión y escrutinio el artículo 19g de la LOREG regula que la Junta Electoral Central aprobara los modelos que permitan la expedición momentánea de las copias necesarias "mediante documentos autocopiativos y otros procedimientos análogos". En este aspecto se ofrece la posibilidad de utilizar métodos informáticos.

La utilización de los medios informáticos se aplica a la administración de la mesa [4] para facilitar la elaboración de las distintas actas, impresión de justificantes, búsqueda más rápida del votante en el censo o la identificación mediante el DNI, se consigue una automatización del proceso.

Finalmente, las elecciones a las Asambleas Autonómicas se regulan por la legislación específica de cada Comunidad, teniendo en cuenta que ciertas ordenanzas de la LOREG son aplicables a estos procesos. El País Vasco es la primera y la única comunidad autónoma en regular el voto electrónico [5] en unas Elecciones al Parlamento, se realizaron estudios conjunto los gobiernos de Bélgica y Brasil, como fruto de esos estudios se llevó a cabo la Ley 15/1998[6], de 19 de junio 1998, de modificación de la Ley 5/1990, de 15 de junio de 1990, de Elecciones al Parlamento Vasco, donde se recoge en el Capítulo X el "Procedimiento de la votación electrónica". Se concreta en el apartado 132bis que el voto electrónico está compuesto por los siguientes elementos: tarjeta con banda magnética, urna electrónica, pantalla de votar, cabina electoral y el software electoral.

[3] http://www.juntaelectoralcentral.es/cs/jec/loreg/contenido?packedargs=idContenido=547083
[4] http://www.euskadi.eus/web01-a2haukon/es/contenidos/informacion/w_be_cae/es_def/index.shtml
[5] http://www.euskadi.eus/web01-a2haukon/es/contenidos/informacion/w_be_eusk_ant/es_def/index.shtml
[6] http://www.legegunea.euskadi.eus/x59-preview/es/contenidos/ley/bopv199803142/es_def/index.shtml

CAPÍTULO 4
Diseño de Evotebox

En este capítulo se va a presentar la arquitectura de Evotebox y las etapas que compone la vida de una votación que se utiliza Evotebox ya que a lo largo de la creación, desarrollo y finalización intervienen distintos elementos necesarios para su funcionamiento.

4.1 Módulos de Evotebox

Evotebox se ha diseñado de forma que sea lo más parecido posible a una votación tradicional, de esta forma el votante está familiarizado con los procedimientos habituales y el uso del nuevo sistema es más fácil de comprender y utilizar.

El sistema se compone de tres módulos principales y cada uno de ellos tiene un funcionamiento distinto:

- Módulo de identificación: el/la votante se identifica mediante el DNI en la urna digital y obtiene la tarjeta de voto.
- Módulo de votación: en este módulo el/la votante realiza la votación que se guarda en la tarjeta de voto.
- Módulo de consignación de voto: finalmente el votante, previa identificación del DNI deposita su voto en el módulo y recoge el recibo de voto en papel.

Estos son los tres módulos que componen el sistema de votación, además existen diferentes procedimientos para la creación de la votación, recuento de votos y para la realización de una auditoria externa.

4.2 Configuración de la votación

Como se ha mencionado anteriormente Evotebox tiene un procedimiento para la creación de la votación, donde el encargado de la votación configurará todos los elementos necesarios para su correcto funcionamiento, los elementos más importantes son:

- Aplicación de creación de la votación: para el desarrollo de la votación es necesaria información relevante como el censo, propuestas de voto, claves de cifrado, etc. Esta aplicación se encarga de generar todos los datos necesarios y guardarlos en dispositivos USB.
- Dispositivos USB: contienen la información de configuración de los módulos.

- Tarjeta de interventor: para asegurar el correcto desarrollo de la votación es necesaria la figura del interventor, este tendrá una tarjeta NFC maestra con la que podrá apagar, reiniciar o terminar la votación.

Con estos tres elementos se puede configurar el sistema Evotebox:

1. Preparación de la votación: es este estado inicial los módulos se encuentran sin configurar, el/la encargado/da de la votación configura una votación con los siguientes elementos:
   - Censo.
   - Claves de cifrado, estas claves son necesarias para el cifrado de las bases de datos.
   - Archivos de información de la votación en formato JSON con las propuestas y tipo de votación.
2. Configuración de las urnas: la información se almacena en un usb, que se conecta a cada uno de los módulos principales, el software se encarga de inicializar cada una de las urnas.

4.3 Auditoría de la votación

Para realizar la auditoria del sistema se dispone de las tarjetas de memoria de los módulos principales empleados en la votación y el código disponible en el repositorio público del proyecto, debido a ello cualquier ciudadano/na puede analizar el código para comprobar su funcionamiento y a través de las tarjetas de memoria la auditoria confirmaría su funcionamiento.

4.4 Etapas en la votación

En este apartado se detallan las etapas necesarias para la realización de la votación correctamente, el estado de partida es el final de la etapa de configuración del sistema.

1. Inicio de la votación: una vez configurado el módulo, la votación puede comenzar y aparecerá la pantalla inicial en cada uno de los módulos.
2. Desarrollo de la votación: el interventor tendrá la capacidad con la tarjeta de interventor de reiniciar los módulos si hay algún problema. Cada vez que se reinicie el módulo será necesario el dispositivo USB con los archivos de configuración.
3. Fin de la votación: el interventor utiliza la tarjeta para cerrar la votación y poder obtener el recuento de votos, además se cifra la base de datos con los resultados en el tercer módulo y se borran todos los datos no útiles.

4.4.1. Módulo de identificación

Es el primer módulo donde el votante se identifica y obtiene la tarjeta de voto cifrada, en este primer módulo el votante introduce el DNI en la ranura a la izquierda donde la cámara reconoce el DNI e identifica al votante con la información del censo, si se produce un error en la identificación el votante puede escribir en la pantalla del módulo sus datos.

Una vez identificado, el módulo graba en la tarjeta de votación las claves necesarias por NFC para que los siguientes módulos la puedan escribir y leer correctamente. Una vez obtenida la tarjeta de voto, el votante retira el DNI y pasa al siguiente módulo.

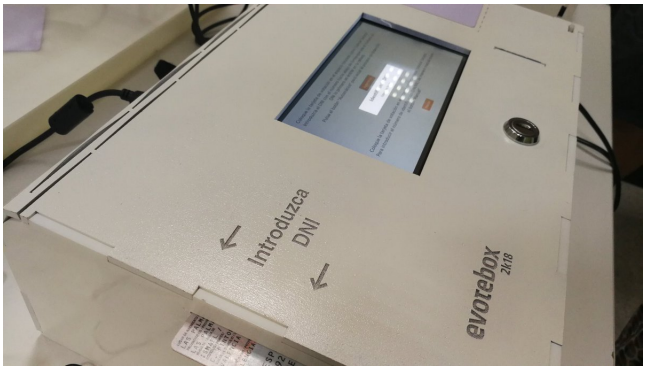

Figura 4.1: Módulo de identificación

4.4.2. Módulo de votación

Este módulo es donde se realiza la votación, el votante, con la tarjeta de voto del módulo de identificación, deposita la tarjeta en el lector NFC del módulo, una vez depositado se habilita la pantalla para la elección de las propuestas.

Finalmente deberá confirmar su selección y se escribirá en la tarjeta NFC la información del voto cifrado con las claves de la votación generadas por la aplicación de creación de la votación.

Una vez realizada la votación el votante puede avanzar al siguiente módulo y finalizar el proceso.

Figura 4.2: Modulo de votación

4.4.3. Módulo de consignación del voto

En el módulo de consignación del voto el votante deposita la tarjeta de voto en el lector NFC y el DNI del votante para su identificación, la aplicación comprueba si el votante ya ha votado si no puede continuar y el voto se guardará en la base de datos.

Finalmente, una vez guardado en la base de datos, la tarjeta de voto se puede depositar en la urna y finalizará el proceso de votación.

Figura 4.3: Módulo de consignación del voto

4.5 Diseño detallado

A continuación, se describe el diseño detallado del sistema de votación Evotebox, primero se especifica la tecnología hardware común en los tres módulos, añadiendo los componentes específicos para cada módulo. Finalmente se detalla el software necesario para la realización de la aplicación de control de la votación.

4.5.1. Hardware

Los componentes hardware que tienen en común los tres módulos son los siguientes:

- Cable USB a micro USB x3
- Cables jumper x18
- Splitter x3
- Cable alargador USB
- Ventiladores x6 (2 para cada módulo)
- Transformador de voltaje x3
- Lector NFC/RFID PN532 Arduino x3
- Regleta x3
- Raspberry PI 3 Model B+ x3
- Pantalla TFT táctil de 7" con placa de control x3

Además para los 3 módulos se utilizan diferentes componentes específicos:

- Módulo 1: Cámara Rapsberry Pi V2 8MP.
- Módulo 3: Cámara Rapsberry Pi V2 8MP, Flash led, Mini reloj tiempo real DS3231.

4.5.2. Software

La aplicación web está escrita en Django versión 1.11, y se basa en el patrón de diseño Modelo-Vista-Template, donde los templates HTML tienen asociados una vista con la lógica de la aplicación y Django proporciona que todas las vistas puedan accederse a través de la url.

La base de datos utilizada para guardar los datos del censo y los resultados de la votación es SQLite3 con la librería oficial de Python para su uso, para la comunicación con el lector NFC Arduino PN532 a través de SPI se utiliza la librería no oficial que actualmente se encuentra obsoleta Arduino Python PN532.

Para el reconocimiento del dni se utiliza la librería pytesseract 0.2 y mediante la librería picamera se obtienen las imágenes de la cámara conectada.

La aplicación de creación de la votación es una página estática con un código HTML y diferentes scripts js para la creación de las claves, el guardado del censo y la creación de la configuración de la votación.

4.6 Tecnología utilizada

Para comprender las vulnerabilidades que se pueden encontrar en el sistema Evotebox se necesita detallar cada una de las tecnologías implicadas en las urnas digitales, por ello a continuación, se definen los conceptos necesarios para entender el análisis de seguridad realizado.

4.6.1. RFID

La tecnología RFID [1] permite la comunicación inalámbrica entre dos dispositivos, comúnmente llamados lector y etiqueta o tarjeta RFID, estos dispositivos pueden almacenar información y transmitirla a través de ondas de radio. Esta tecnología empezó a utilizarse para la identificación de aviones aliados en la Segunda Guerra Mundial.

Figura 4.4: Logo RFID

Este tipo de tecnologías se agrupan dentro de las llamadas Auto ID o identificación automática junto con los códigos de barras, reconocimiento biométrico, reconocimiento de voz, etc.

Un sistema RFID se compone de los siguientes componentes:

[1] https://es.wikipedia.org/wiki/RFID

- Etiqueta o tarjeta RFID: contiene unas antenas capaces de responder a peticiones por radiofrecuencia y transmitir la información almacenada en el chip.
- Lector de RFID: contiene una antena para la transmisión de ondas electromagnéticas, transmite periódicamente señales para descubrir etiquetas y realizar la comunicación. También se encarga de enviar la información y pasarla al subsistema de procesamiento de datos.
- Subsistema de procesamiento de datos: recibe la información del lector y la procesa.

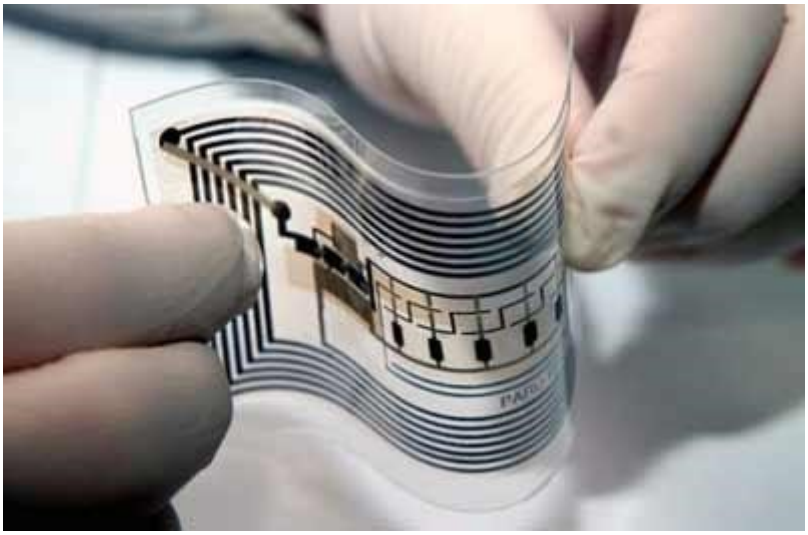

Figura 4.5: Circuito RFID

Además, existen tres tipos diferentes de etiquetas o tarjetas RFID:

- Etiquetas pasivas: no tienen alimentación eléctrica, la señal transmitida por los lectores induce una corriente eléctrica suficiente para que pueda transmitir una respuesta.
- Etiquetas activas: poseen su propia alimentación eléctrica que utilizan para dar corriente y transmitir una respuesta al lector.
- Etiquetas semiactivas: también poseen una alimentación propia, pero en este caso se utiliza para alimentar el propio chip, no para transmitir, en este caso la energía transmitida por el lector es la utilizada para transmitir la señal.

4.6.2. NFC

NFC es el acrónimo de "Near Field Communication" [2], se trata de una tecnología de comunicación inalámbrica de corto alcance y alta frecuencia que permite el intercambio de datos entre dos dispositivos cercanos. Está diseñado para trabajar sobre RFID permitiendo intercambios de datos más complejos entre los dispositivos.

Se comunica en la frecuencia de 13,56 Mhz, esta frecuencia es de libre uso por lo que no se aplica ninguna restricción legal como en otras frecuencias utilizadas para la televisión o la radio. La distancia máxima teórica de transmisión son 20 cm y su tasa de transferencia puede llegar a los 106,212, 424 u 848 kbit/s.

Figura 4.6: Logo NFC

Esta tecnología está especificada bajo los estándares NFC que cubren los protocolos de comunicación y formatos de intercambio de datos, basados en ISO-14443 (RFID), NFCIP-1(ISO 18092) y NFCIP-2 (ISO 21481). La regularización de los estándares la realiza la organización NFC Forum, creada en 2004 por Nokia, Philips y Sony, aunque en la actualidad se incluyen Google, Apple, Microsoft, Huawei, Samsung, Mastercard o Visa, entre otras.

Figura 4.7: Foro NFC FORUM

En la actualidad el desarrollo de la tecnología se enfoca en los dispositivos móviles y en el comercio electrónico debido a su velocidad de comunicación y a la gran variedad de aplicaciones que se puede aplicar su corta distancia de transmisión. [11]

Además de regular los estándares NFC Forum define sus objetivos:

- Desarrollar sus especificaciones y comprobar los mecanismos que aseguran una consistencia, confiabilidad en las transacciones de todos los modos de NFC.

[2] https://es.wikipedia.org/wiki/Near_field_communication

- Fomentar el desarrollo de la tecnología en la industria.
- Educar a las empresas, proveedores de servicio y desarrolladores sobre los beneficios de NFC.
- Asegurar que los productos con la marca NFC cumplen con las especificaciones determinadas por el NFC Forum.

Funcionamiento

Se disponen de dos modos de comunicación similares a los tipos de etiquetas o tarjetas RFID antes mencionados:

- Activo: los dispositivos tienen su propia alimentación de energía y generan su propio campo de RF* permitiendo la iniciación de la comunicación.
- Pasivo: uno de los dispositivos inicia la comunicación generando el campo de RF y el transmisor responde mediante la modulación del campo, por lo que no necesita tener alimentación de energía.

Basada en la posibilidad de interacción, NFC Forum ha definido la siguiente arquitectura[12].

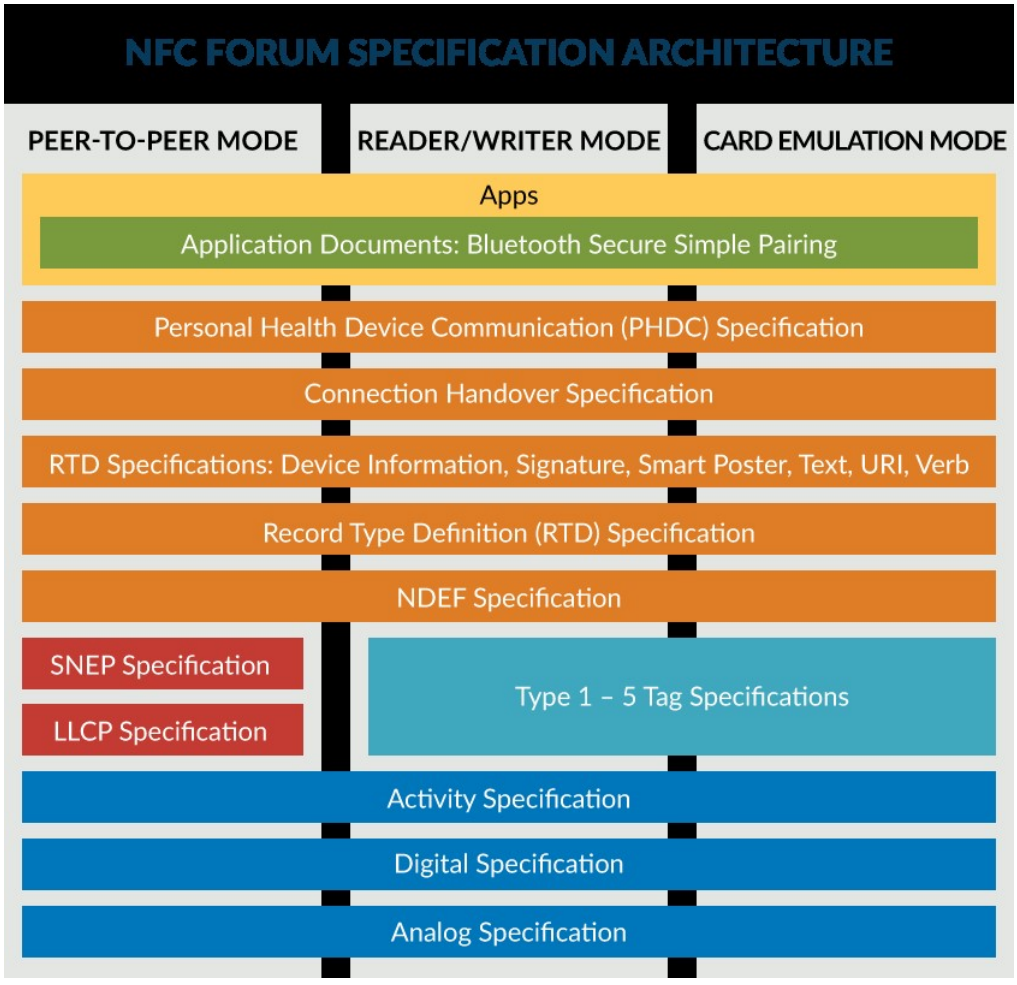

Figura 4.8: Especificación arquitectura NFC

En esta arquitectura se definen tres modos de operación que los dispositivos NFC deben cumplir para cumplir con la especificación de NFC Forum:

- Modo reader/writer: define que el dispositivo NFC es capaz de leer las tarjetas y poder escribir sobre ellas.
- Modo Peer-to-Peer: define que dos dispositivos NFC pueden intercambiar datos en ambas direcciones, por ejemplo, la compartición de los datos de configuración de una conexión WiFi.
- Modo Card Emulation: define que el dispositivo NFC se muestra como una etiqueta RFID cuando están en el campo de otro dispositivo NFC o RFID.

Especificaciones de NFC Forum

NFC Data Exchange Format (NDEF)

Define el formato del mensaje transmitido común a todos los dispositivos compatibles con NFC, es uno de los principales cambios que se añaden al estándar de RFID. Cada mensaje puede contener uno o más NDEF campos, y cada campo tiene su propio campo tipo, un ID único, tamaño, y la carga útil del dato.

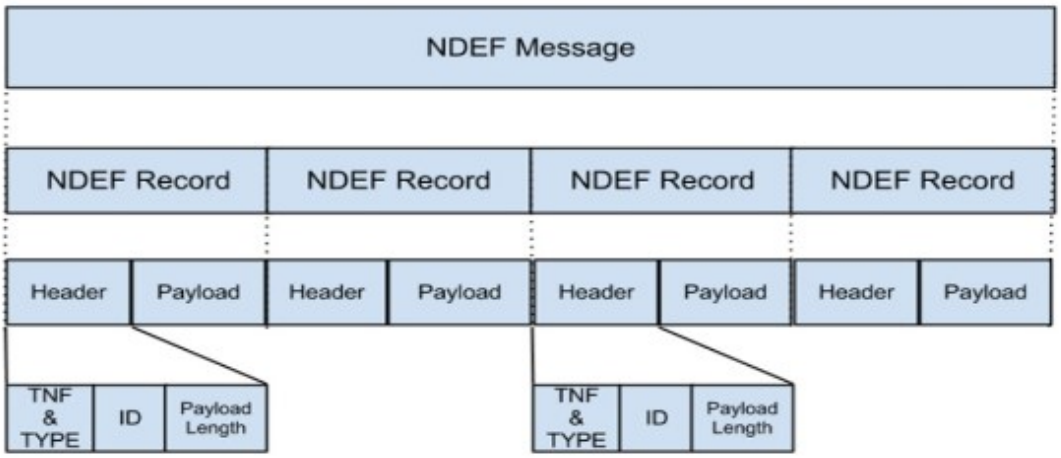

Figura 4.9: Formato mensaje NDEF

NFC Record Type Definition (RTD)

Define el formato y las reglas para crear los registros estándar del formato NDEF que pueden ser usados por las aplicaciones NFC. NFC Forum establece estas cuatro RTD específicas:

- NFC Text RTD: defina una forma de almacenar cadenas de texto.
- NFC URI RTD: define una forma de almacenar URIs.
- NFC Smart Poster RTD: define un formato para almacenar URLs, SMSs o números de teléfono.
- NFC Generic Control RTD: define una forma simple para que el dispositivo NFC "origen" solicite una acción específica a un dispositivo NFC "destino".

NFC Tag Types

NFC Forum ha elegido los cuatro tipos de etiquetas (tags) más extendidos, y los ha definido como los tipos de tags cuyo soporte es obligatorio para los dispositivos compatibles con la arquitectura de NFC Forum, de esta forma asegura una interoperatividad entre dispositivos NFC de diferentes fabricantes.

	Tipo 1	Tipo 2	Tipo 3	Tipo 4
Interfaz RF	ISO 14443 A-2	ISO 14443 A-2	FeliCa (ISO 18092, modo de comunicación pasivo a 212 Kbps)	ISO 14443-2
Inicialización	ISO 14443 A-3	ISO 14443 A-3	FeliCa (ISO 18092, modo de comunicación pasivo a 212 Kbps)	ISO 14443-3
Velocidad	106 Kbps	106 Kbps	212 Kbps	106-424 Kbps
Protocolo	Conjunto de comandos específicos	Conjunto de comandos específicos	Protocolo FeliCa	Comandos ISO 14443-4, ISO 7816-4
Memoria	Hasta 1 KB	Hasta 2 KB	Hasta 1 MB	Hasta 64 KB
Costo (dependiente de la memoria)	Bajo	Bajo	Moderado	Moderado
Casos de uso	Tags con memoria reducida para aplicaciones simples		Tags flexibles con mayor cantidad de memoria que permiten múltiples aplicaciones	

Figura 4.10: Tipos de NFC Tag

4.6.3. Raspberry Pi

Es un ordenador de placa reducida u ordenador de placa simple (SBC) de bajo coste, es desarrollado por la Fundación Raspberry Pi con el objetivo de enseñar programación y electrónica en las escuelas. Aunque su hardware sea un producto de marca registrada, se permite su uso libre tanto a nivel particular como a nivel educativo, debido a ello se ha convertido en la placa más vendida para proyectos de particulares. [3]

En cambio, su software, si es de código abierto, permitiendo la libre distribución y desarrollo para todo el mundo. Su sistema operativo oficial se denomina Raspbian, una versión adaptada de Debian. Actualmente permite el uso de distintos sistemas operativos, incluyendo una versión de Windows 10 preparada para su uso en dispositivos con menor capacidad de CPU y memoria.

Figura 4.11: Placa Raspberry Pi

Hardware

Existen diferentes modelos de Raspberry Pi, el modelo actual que más se utiliza es el Raspberry Pi 3 Model B+ y tiene las siguientes características:

- Procesador: Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC.
- Frecuencia de reloj: 1.4 GHz.
- Memoria: 1GB LPDDR2 SDRAM.
- Conectividad inalámbrica:
  - 2.4GHz / 5GHz.
  - IEEE 802.11.b/g/n/ac.
  - Bluetooth 4.2, BLE.
- Conectividad de red: Gigabit Ethernet over USB 2.0 (300 Mbps de máximo teórico)
- Puertos:
  - GPIO 40 pines
  - HDMI
  - 4 x USB 2.0
  - CSI (cámara Raspberry Pi)
  - DSI (pantalla tácil)

[3] https://es.wikipedia.org/wiki/Raspberry_Pi

- Toma auriculares / vídeo compuesto
- Micro SD
- Micro USB (alimentación)
- Power-over-Ethernet (PoE)

Además, la Fundación Raspberry Pi ha sacado otra gama de placas denominadas Raspberry Pi Zero, más pequeñas y menos potentes, pero de un gasto energético y precio menor.

El modelo utilizado en las urnas digitales Evotebox son las Raspberry Pi 3 Modelo B+, por lo tanto, de ahora en adelante se referirá a este modelo en concreto cada vez que se mencione Raspberry Pi

Software

Entre los sistemas operativos existentes el utilizado para el diseño de la urna digital es DietPi por lo que me centraré en comentar los aspectos básicos de la distribución DietPi.

Se trata de una distribución basada en Debian 8 Jessie de 64 bits y es creada por Daniel Knight, tiene muchas ventajas, pero las principales que sirven para el presente trabajo son:

- Ligereza en el consumo de recursos.
- Optimizada para un uso mínimo de CPU y RAM.
- Software pre-instalado mediante scripts.
- Logs configurados y pre-instalados.
- Instalación en entornos virtuales como VirtualBox o VMware.

4.6.4. Arduino

Arduino [4] es un projecto de hardware y software distribuidos bajo licencia Pública General Reducida de GNU (LGPL) permitiendo la distribución y fabricación de placas Arduino y software por todo el mudo. Fue creado en el Instituto Ivrea de Italia en 2005, actualmente el principal distribuidor de componentes electrónicos Arduino es Adafruit.

Consiste en un sistema hardware y un entorno de desarrollo (IDE) para su programación. Incluye todo tipo de hardware de creación de sistemas electrónicos, desde robótica hasta impresoras 3D.

Figura 4.12: Logo Arduino EEUU

Figura 4.13: Logo Arduino Europa

Existen multitud de placas Arduino pero el hardware utilizado para el Sistema de votación electrónica es el controlador NFC/RFID PN532 proporcionado por Adafruit, es el chip más utilizado para la lectura de dispositivos tanto NFC como tags RFID.

Dispone de la interfaz de comunicación I2C o SPI, mediante estas interfaces se asegura una conexión con la placa Raspberry Pi utilizada. Soporta la librería de código abierto Libnfc que permite el desarrollo de aplicaciones sin tener que lidiar con la comunicación a nivel bajo de NFC.

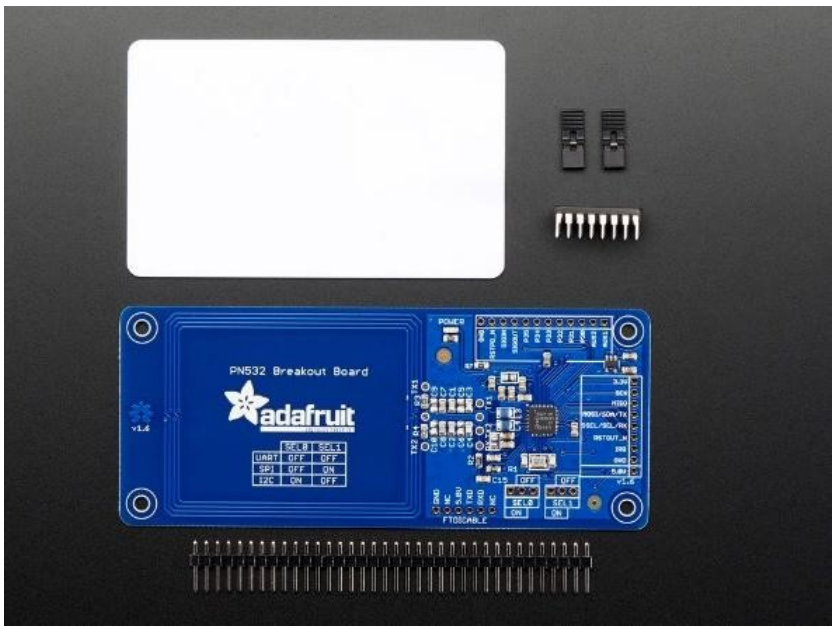

Figura 4.14: Place controlador NFC/RFID PN532 de Adafruit

[4] https://es.wikipedia.org/wiki/Arduino

La librería utilizada en las urnas digitales es la proporcionada por Adafruit y proporciona una librería en el lenguaje Python diseñada específicamente para acceder al chip PN532 da través de una conexión SPI desde una Raspberry Pi.

CAPÍTULO 5
Análisis de las vulnerabilidades

En este capítulo se presenta el análisis de la seguridad del sistema de votación electrónica Evotebox. A partir de la arquitectura y el diseño del sistema de votación se detallan las vulnerabilidades que afectan las tecnologías utilizadas en el desarrollo, explicando en qué consisten dichas vulnerabilidades.

5.1 Vulnerabilidades NFC

La seguridad es uno de los principales objetivos de la tecnología NFC, por ello se han desarrollado tantos estándares y mecanismos para proteger los datos, y existe el NFC Forum para asegurar una calidad en las implementaciones[1]. A pesar de ello existen una gran variedad de ataques a NFC.

Según la página oficial de NFC Forum, NFC debe ser inherentemente seguro debido al corto rango de comunicación y a las propiedades de la modulación RF, no obstante, al ser una tecnología de comunicación por radiofrecuencias siempre se podrá interferir en la transmisión a cierto rango, determinado por la capacidad de señal de la antena RFID/NFC.

Existen también una serie de inhibidores de frecuencia o jammers, estos dispositivos no eliminan la onda de radio, sino que emiten interferencias a modo de ruido sobre una banda en concreto. La emisión de las ondas provoca que los dispositivos a la escucha no puedan recibir la transmisión de datos realizando una denegación de servicio.

En definitiva, existen 3 problemas principales a los que una implementación que utilice la tecnología NFC se debe proteger[14]:

- Escucha secreta o eavesdropping.
- Retransmisión o relay attack
- Modificaciónd del dato.

El sistema Evotebox, como se ha detallado en el apartado 4 se utilizan los tags MIFARE 1K y 4K, y el lector Adafruit PN532 RFID/NFC, en las explicaciones de los ataques se asume que se utiliza esta tecnología como víctima.

A continuación, se explica que vulnerabilidades de NFC afectarían al sistema de votación electrónica Evotebox y además se proporcionan diferentes ejemplos de explotación de la vulnerabilidad.

[1] https://nfc-forum.org/our-work/nfc-forum-security-faqs/

5.1.1. Escucha secreta o eavesdropping

Este problema de seguridad radica en la posibilidad de escuchar la comunicación entre un tag NFC y un lector NFC, según el estándar del NFC Forum tan solo se puede escuchar la transmisión a un máximo de 10 a 15 cm pero existen diferentes estudios[13] en los que se ha conseguido aumentar la distancia máxima hasta 1 metro con el modo pasivo y los 10 metros si se utiliza el modo activo.

La distancia también puede variar dependiendo de la capacidad de las antenas utilizadas por el atacante, ya que tan solo se requiere una señal lo suficientemente fuerte para poder escuchar la comunicación. Esta señal también varia si existen interferencias físicas entre el atacante y los dispositivos, como por ejemplo muros, coches, camiones, etc.

Figura 5.1: Captura de señal inalámbrica

En el sistema Evotebox el atacante realizaría el ataque mediante el uso de un sistema de SDR (Radio definida por software, Software defined Radio) y una antena RFID/NFC. Estas antenas al componerse de un inductor[2] se pueden construir de forma casera.

El atacante se situaría con el equipo a cierta distancia de la votación (dependiendo de la capacidad de la antena RFID/NFC) y mientras se desarrolle la votación puede ir almacenando los votos que se realizan, además se podría correlacionar un voto a un votante si la información de un votante y el voto se transmiten en un corto periodo de tiempo, esta escucha puede inducir a fallos debido a que múltiples personas pueden estar votando al mismo tiempo.

5.1.2. Retransmisión(relay attack)

Se trata de un ataque denominado "hombre en el medio"(man-in-the-middle), el atacante intercepta la comunicación igual que en el ataque de escucha secreta, pero esta vez cuando un mensaje es transmitido entre los dispositivos el atacante lo intercepta y lo redirige al exterior, también se puede modificar la información, pero la variante de este ataque se trata en la ex filtración de la información no en la modificación.

[2]https://es.wikipedia.org/wiki/Inductor

El atacante utilizaría los mismos medios para la obtención de la información solo que esta vez el atacante redirigiría los datos a otras organizaciones y no los almacenaría.

En el sistema Evotebox un atacante puede ex filtrar la información a una entidad fuera de la votación, con ello diferentes entidades pueden conocer los detalles de la votación sin necesidad de encontrarse físicamente en el lugar de la votación. De este modo medios de comunicación o los implicados en la votación pueden obtener información valiosa para el desarrollo de las siguientes votaciones.

Mediante este sistema se puede almacenar los votos para publicarlos a la red o venderlos a diferentes organizaciones como el caso de Cambrigde Analytica donde Facebook utilizó los datos de los usuarios para la campaña del candidato republicano a la presidencia de los Estados Unidos, Donald Trump.

5.1.3. Modificación del voto

En este ataque se puede modificar la información de comunicación según la voluntad del atacante, se utilizan los mismos medios para la obtención de la información que en los dos anteriores ataques. En este caso existen 4 posibilidades respecto a la modificación de la información:

- Denegación de servicio: El atacante utiliza un inhibidor de señal o jammer para generar ruido, de tal modo la información no se podría leer, afectando a la disponibilidad del sistema.

- Destrucción de la información: el atacante puede emitir en una determinada frecuencia para provocar efectos de superposición en la comunicación NFC, anulando los mensajes de configuración NFC y afectando a la disponibilidad del sistema.

- Modificación de la información: un atacante puede utilizar la modulación de la señal para manipular los paquetes. En este ataque se depende de la codificación que se utilice en la modulación y si la información transmitida se encuentra cifrada por software.

- Inserción de la información: el atacante genera paquetes aceptados por el lector, este ataque afecta a la integridad del sistema.

En el sistema Evotebox la información de los tags NFC se encuentra cifrada por software, debido a ello para que el atacante pueda modificar correctamente la información y que el sistema lo acepte debe reproducir el esquema de cifrado utilizado, a pesar de ello el atacante podría realizar un proceso de ingeniería inversa para determinar el esquema de cifrado y enviar datos correctos. En cambio, el proceso de votación se realiza en un espacio temporal corto, y el cifrado utilizado en Evotebox AES-256 necesita de cierto tiempo computacional para romper la clave, por lo tanto, en este apartado se contempla la denegación de servicio o la destrucción de la información como ejemplos de ataque posibles.

En los dos ataques mencionados el atacante puede afectar a la disponibilidad del sistema, por lo que se podría convertir en una pérdida de confianza en las votaciones electrónicas y por lo tanto afectando a uno de los pilares necesarios para el desarrollo de las votaciones.

5.2 Vulnerabilidades de hardware

En seguridad la mayor parte de las vulnerabilidades estudiadas son las relacionadas con el software, sin embargo, las vulnerabilidades de hardware suelen ser las más comunes, como la falta de actualización de los equipos o la exposición de interfaces de comunicación.

En consequencia, en el sistema Evotebox se ha procurado exponer lo mínimo posible al exterior y además se adopta una política de actualización de hardware, por lo tanto, la superficie de ataque disminuye. Sin embargo, para realizar la configuración de la urna se utiliza un dispositivo USB y por tanto se requiere de un puerto expuesto, además la utilización de Raspberry Pi como ordenador dentro de la urna implica existe interfaces que también se pueden utilizar para realizar diferentes ataques.

5.2.1. Implantación USB

Esta vulnerabilidad es una de las más antiguas, pero continúa siendo uno de los vectores de ataques más comunes, afecta a la interfaz USB. La interfaz se utiliza para la conexión de dispositivos de almacenamiento y de periféricos en los sistemas, estos dispositivos contienen un firmware que define su ejecución y configuración cuando se conectan a la interfaz.

Existen estudios [15] donde a través de un USB con firmware modificado simular un periférico que puede ejecutar código arbitrario en cualquier dispositivo que se ha conectado. Asi mismo, se pueden implementar diferentes técnicas para enmascarar su comportamiento antes de ejecutar el código.

Figura 5.2: USB Rubber Ducky de Hak5.

En el caso de Evotebox, un atacante podría introducir un USB con un firmware modificado en el puerto expuesto de la carcasa, mediante este proceso se podría acceder a cualquier dato almacenado en la urna, y también si el atacante conoce la estructura interna de los archivos de configuración o el código fuente podría modificar la lógica de la urna digital.

5.2.2. Modificación de la tarjeta MicroSD

Las Raspberry Pi utiliza una tarjeta MicroSD donde se almacena el sistema operativo y se utiliza como disco de almacenamiento principal. Debido a ello, un atacante puede cambiar la tarjeta MicroSD por una propia modificada, si consigue acceder fisicamente a la Raspberry Pi.

Para que el ataque no afecte la disponibilidad del sistema, la tarjeta cambiada debe simular el funcionamiento de la tarjeta original, de este modo el ataque puede no ser detectado hasta que se revise posteriormente el sistema.

Una vez cambiada la tarjeta MicroSD y simulado el funcionamiento real del sistema el atacante tiene acceso completo a la información de la votación y como la Raspberry Pi tiene interfaz WiFi se puede conectar a una red preparada para exfiltrar la información a tiempo real.

5.2.3. Ataque por interferencia Van Eck

Es un tipo de ataque muy específico que se utiliza para espiar el contenido de un monitor LCD y CRT mediante la detección de las emisiones electromagnéticas, este ataque fue el que utilizo el gobierno de Holanda como argumento para prohibir el uso de las máquinas de votación por no cumplir las garantías esablecidas.

Para realizar el ataque[16] es necesario un hardware muy específico, antenas lo suficientemente potentes para captar la señal que el monitor LCD de la Raspberry Pi tiene conectado y un software de conversión de las señales de radio en información útil para el atacante.

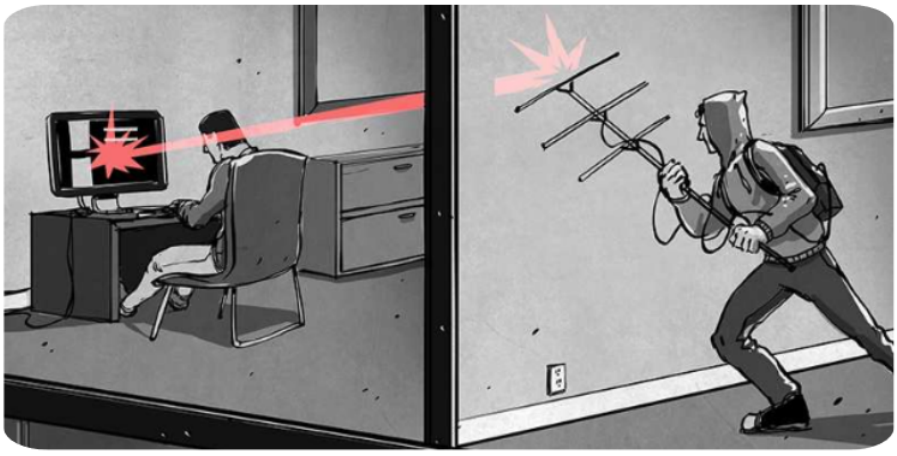

Figura 5.3: Ataque por interferencia Van Eck.

Una vez obtenidos los componentes necesarios el atacante puede colocarse a cierta distancia de la votación (dependiendo de la potencia de la antena), en este caso la pantalla LCD más interesante para capturar los datos es la pantalla del módulo de votación ya que en esta pantalla se eligiran las diferentes propuestas. Una vez obtenidos los datos de las propuestas capturadas, el atacante puede filtrar la información a organizaciones externas.

5.3 Vulnerabilidades de software

Las vulnerabilidades de software son fallos de seguridad en la aplicación software o en el sistema operativo mediante el cual un atacante puede llegar a comprometer la seguridad de todo el sistema sobre el que se ejecuta.

Debido a que existen una gran multitud de vulnerabilidades, diferentes organizaciones han creado bases de datos con la información de vulnerabilidades de software conocidas, entre ellas la base de datos más popular y con más de 75.000 registros es la National Vulnerability Database [3] mantenida por el gobierno de Estados Unidos. En este repositorio se utiliza el estándar de nomenclatura de vulnerabilidades CVE (Common Vulnerabilities and Exposures) [4] para facilitar el intercambio de información entre diferentes herramientas.

También existen diferentes organizaciones dedicadas a combatir las causas por las que el software es inseguro, entre estas organizaciones se encuentra OWASP (Open Web Application Security Project) [5] su comunidad está formada por empresas, organizaciones y particulares a lo largo del mundo, donde se trabaja creando artículos, metodologías, documentación, herramientas y tecnologías que se pueden liberar y utilizar gratuitamente por cualquiera. Como se ha detallado anteriormente el sistema Evotebox utiliza como aplicación web Django [6] sobre el sistema operativo DietPi basado en Debian OS para Raspberry Pi, según la página oficial de Django existen diferentes niveles de seguridad según las vulnerabilidades. [17]

Alta

- Ejecución de código.
- Inyección SQL.

Moderada

- Cross site scripting (XSS).
- Cross site request forgery (CSRF).
- Ataque Denial-of-service (DOS).
- Autenticación rota.

Baja

- Exposición de datos sensibles.
- Manejo de sesiones roto.
- Redirecciones no válidas.
- Fallos de opciones de configuración.

A continuación, se explican 3 casos que pueden afectar a la aplicación web del sistema Evotebox.

[3] https://nvd.nist.gov/
[4] https://cve.mitre.org/
[5] https://www.owasp.org/index.php/Main_Page
[6] https://www.djangoproject.com/

5.3.1. Cross site scripting (XSS)

Este tipo de vulnerabilidad permite la inyección de código en el navegador de los usuarios, es comúnmente explotado a través de guardar código malicioso en la base de datos donde la información va a ser mostrada al usuario o haciendo que el usuario pinche un enlace que causa que el navegador ejecute código JavaScript, robando la información del usuario o provocando que la información introducida por el usuario sea modificada. Se pueden originar desde cualquier dato origen no confiable, como cookies o servicios web, donde los datos no se encuentran suficientemente sanitizados antes de incluirse en la página web.

En Django existen templates que te protegen de la mayoría de los ataques XSS, sin embargo, contienen los caracteres específicos de escape mediante los cuales se genera contenido para la página web, estos caracteres si no son usados correctamente permiten que se inyecte el código malicioso.

Por ejemplo, al utilizar este código de ejemplo: [7]

```
<input class={{ var }}>...</input>
```

Si la variable var se asigna como:

```
'class1 onmouseover=javascript:func()'
```

El resultado puede ser una ejecución de código maliciosa en caso de que el navegador renderice incorrectamente el HTML, en este caso citando el valor del atributo se corregiría o utilizando las etiquetas del template disponibles con django como safe o make_safe permiten interpretar correctamente la entrada del usuario.

En Evotebox existe el riesgo de un ataque XSS al introducir los datos del DNI en el primer módulo, debido a que se expone el usuario a que introduzca datos no confiables que la aplicación tendrá de tratar, este código malicioso puede mostrar la información que se encuentre en el disco duro en ese momento.

5.3.2. Exposición de datos sensibles

Cuando el usuario introduce cualquier información en una aplicación web se asume que el servidor protegerá los datos introducidos, pero aun así se pueden aprovechar malas configuraciones o vulnerabilidades de la aplicación web como el cross site scripting (XSS) para exponer los datos al público u organizaciones privadas.

Por ejemplo, en la aplicación Django por defecto al inicio de la creación de la aplicación se ajusta la variable DEBUG = TRUE , esto es útil cuando se despliega la aplicación para desarrollo, sin embargo, si no se desactiva el modo debug la aplicación puede mostrar información relevante sobre el entorno en el que se ejecuta e incluso los ajustes de configuración del fichero settings.py.

Como medida de seguridad extra, Django no incluye información sensible que contenga los siguientes nombres:

- API
- KEY
- PASS

[7] https://docs.djangoproject.com/en/2.2/topics/security/

- SECRET
- SIGNATURE
- TOKEN

En el caso de que se despliegue con estos fallos de configuración, el sistema Evotebox será vulnerable a la exposición de datos sensibles, y con ello cualquier atacante puede obtener información relevante de la votación.

5.4 Vulnerabilidades humanas

Estas vulnerabilidades se refieren a los daños que las personas pueden causar al sistema, muchas veces existen errores o accidentes mediante los cuales la seguridad del sistema puede quedar comprometida, a continuación, detallo el principal problema que se puede enfrentar el sistema de votación electrónica Evotebox.

5.4.1. Ingenieria social

La ingeniería social [8] es una práctica para obtener información confidencial, el acceso a un sitio restringido u obtención de unos privilegios en sistemas de información. El principio de la ingeniería social es que cualquier sistema se puede comprometer debido a que los usuarios son el eslabón más débil.

Esta técnica ha sido ampliamente utilizada a través del teléfono o Internet para engañar a la gente y obtener información o que el usuario entre a una página web maliciosa a través de un enlace engañoso. Permitiendo el secuestro de las contraseñas y posteriormente a el compromiso de todo el sistema a través de una vulnerabilidad dentro del sistema.

En este caso se puede utilizar este tipo de técnicas enviado correos fraudulentos a los componentes de la organización de la votación, con el fin de obtener el acceso a los ordenadores y robar las claves de cifrado de la votación a través de un programa maligno o manipular el censo antes de que se introduzca en el sistema.

Otro ataque muy común seria la obtención de la tarjeta interventor engañando o aprovechando el despiste de alguno de los organizadores que se encuentren físicamente en la votación, el atacante puede manipular los estados del sistema forzando un apagado o un recuento, invalidando los votos ya realizados y evitando que los demás ciudadanos/as voten.

[8] https://es.wikipedia.org/wiki/Ingeniería_social_(seguridad_informática)

CAPÍTULO 6
Propuestas de soluciones

En este capítulo se presentan algunas posibles soluciones a las vulnerabilidades antes planteadas, estas soluciones dependen de como se realiza el desarrollo y cuales son los requisitos que el sistema necesite, por lo tanto tan solo se realiza una aproximación para que a lo largo del desarrollo se puedan obtener mejores soluciones.

- Implementación de un algoritmo de cifrado asimétrico del contenido de las tarjetas NFC.
- Realizar una suma de verificación cada vez que se escriba en las tarjetas NFC y comprobar el valor cada vez que se introduzca la tarjeta NFC en la urna digital.
- Sellado de las urnas físicamente y fijado a un objeto inmóvil en el recinto del centro de votación.
- Uso del sistema de un entorno suficientemente aislado (como una jaula de Faraday[1]) para que no se puedan realizar ataques a través de ondas de radio electromagnéticas.
- Formación de las personas responsables de la votación, en materia de seguridad para evitar los ataques de ingenieria social.
- Utilización de un software que no acepte valores introducidos por el usuario.

[1] https://es.wikipedia.org/wiki/Jaula_de_Faraday

CAPÍTULO 7
Conclusiones

Conseguir la confianza de la ciudadania en la realización de las votaciones electrónicas es un proceso largo y complejo, los electores no deben de albergar ninguna duda que se cumplen los mismos principios y requisitos existentes en las votaciones tradicionales.

Afortunadamente existen diferentes consideraciones de seguridad dictadas por organismos internacionales en las que poder apoyarnos en la implementación de estos sistemas, como las Recomendaciones del Comité de Ministros del Consejo de Europa de septiembre de 2004[18] o los Estandares para los sistemas de voto electrónico aprobados por la Comisión Electoral Federal de los Estados Unidos de America de abril de 2002[19].

Las principales vulnerabilidades detalladas en este trabajo son vulnerabilidades referentes a fallos al realizar una correcta implementación del código de la aplicación como pueden ser los ataques donde se necesita el acceso físico al sistema o vulnerabilidades referentes a la arquitectura de la tecnología NFC.

En este sentido, es importante que la implementación de la solución pueda atender a estos estandares de seguridad mínimos establecidos y siempre hay que tener en cuenta que las nuevas tecnologías siempre implican riesgos asociados. Debido a ello, es necesario conocer las vulnerabilidades que afectan estas tecnologías y así poder poner en práctica planes de respuesta y de mitigación.

Recogiendo lo más importante, para realizar una correcta implementación de la seguridad en los sistemas de votación electrónica como es el caso de Evotebox, es necesario seguir las diferentes consideraciones de seguridad ya establecidas y aprobadas por los organismos internacionales y además realizar un trabajo de investigación de las tecnologías implicadas en la solución para poder mitigar las vulnerabilidades que tengas o que puedan ocurrir.

Finalmente con estas pautas se puede realizar un sistema de votación electrónico que genere confianza en los ciudadanos, consiguiendo respetar los mismos principios que la votación tradicional y avanzar hacia una sociedad donde la ciudadania puede implicarse más en los procesos democráticos de los gobiernos.

Bibliografía

[1] Espinoza, Joaquín Yrivarren. Gobierno electrónico, análisis de los conceptos de tecnología, comodidad y democracia. *YoPublico*, 2009.

[2] Recomendación Rec(2004)11 del comité de ministros del consejo de Europa a los estados miembros sobre los estandares legales, procedimentales y técnicos de los sitemas de votación electrónica, 2018. Consultado en https://www.coe.int/t/dgap/goodgovernance/activities/key-texts/recommendations/E-votingRec_Spanish.asp.

[3] Voluntary Voting System Guidelines Consultado en https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/

[4] Una introducción al voto electrónico: Consideraciones esenciales, 2011. Consultado en https://www.idea.int/sites/default/files/publications/una-introduccion-al-voto-electronico.pdf.

[5] Voting system Reports Collection from U. S. Election Assistance, 2018. Consultado en https://www.eac.gov/voting-equipment/voting-system-reports-collection/.

[6] Defcon 26 Voting Village Report, 2018. Consultado en https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf.

[7] Análisis de factibilidad en la implementación de tecnología en diferentes aspectos y etapas del proceso electoral, 2017. Consultado en http://www.conicet.gov.ar/wp-content/uploads/Analisis_factibilidad_implementacion_tecnologia_proceso_electoral.pdf.

[8] Belleboni, Emilia Pérez, et al. Analysis of electronic and telematic voting systems in binding experiences. *Universidad Politécnica de Madrid*, 2012.

[9] García Soriano, María Vicenta. Una recomendación de las garantías electorales ante las nuevas modalidades de (e-)votación. *Revista de Derecho Electoral*, mayo, 2007.

[10] Ley Orgánica 5/1985, 1985. Consultado en http://www.juntaelectoralcentral.es/cs/jec/loreg/contenido?packedargs=idContenido=546269&letra=J.

[11] Carignano, María Fernanda. NFC (Near Field Communication). *Instituto Universitario Aeronáutico*, 2004.

[12] Especificación de la arquitectura de NFC, 2018. Consultado en https://nfc-forum.org/our-work/specifications-and-application-documents/specifications/.

[13] Thomas P. Diakos, Johann A. Briffa, Tim W. C. Brown, Stephan Wesemeyer. Eavesdropping Near Field Contactless Payments: A Quantitative Analysis. *Computer Laboratory, University of Cambridge*, 2014.

[14] Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema, Consultado en https://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/.

[15] Hacking microcontroller firmware through a USB, Consultado en https://securelist.com/hacking-microcontroller-firmware-through-a-usb/89919/.

[16] TEMPEST attacks against AES, Consultado en https://www.fox-it.com/en/wp-content/uploads/sites/11/Tempest_attacks_against_AES.pdf.

[17] Django's security policies, Consultado en https://docs.djangoproject.com/en/dev/internals/security/.

[18] Committe of Ministers. 11 of the Committe of Ministers to member states on legal, operational and technical standards for e-voting. *Committe of Ministers*, 2004.

[19] Voting System Standards, Testing and Certification, Consultado en http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx.