



Departamento de Matemáticas

MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD

Trabajo de Fin de Máster

EVALUACIÓN DE LA SEGURIDAD EN PUNTOS DE RECARGA PARA VEHÍCULOS ELÉCTRICOS

EVALUATION OF SECURITY IN CHARGING
POINTS FOR ELECTRIC VEHICLES

Autor: Miguel López Soto

Tutor: Ángel Manuel Guerrero Higueras

Cotutor: Adrián Campazas Vega

(Septiembre, 2022)

UNIVERSIDAD DE LEÓN
Departamento de Matemáticas

MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD
Trabajo de Fin de Máster

ALUMNO: Miguel López Soto

TUTOR: Ángel Manuel Guerrero Higueras

COTUTOR: Adrián Campazas Vega

TÍTULO: Evaluación de la seguridad en puntos de recarga para vehículos eléctricos

TITLE: Evaluation of security in charging points for electric vehicles

CONVOCATORIA: Septiembre, 2022

RESUMEN:

Se evaluarán diferentes aspectos en general de la seguridad de los postes del coche eléctrico y se propondrán algunas soluciones a través de su sistema de gestión basadas en el doble factor de autenticación (2FA) y las tecnologías NFC.

Palabras clave: Seguridad; prevención; postes de recarga; doble factor; NFC; RFID;

Firma del alumno:	VºBº Tutor:	VºBº Cotutor:

Índice general

Índice de figuras	v
Índice de tablas	vii
Glosario de términos	viii
Introducción	1
1. Estudio del problema	4
1.1. El contexto del problema	4
1.2. El estado del arte	4
1.2.1. Metodología	4
1.2.1.1. Planificación de búsqueda	4
1.2.1.2. Proceso de búsqueda	5
1.2.1.3. Selección de muestras	6
1.2.1.4. Extracción de datos	7
1.2.2. Resultados	8
1.3. Definición del proyecto	10
1.4. La definición del problema	10
2. Tecnologías NFC y RFID	12
2.1. Diferencias entre NFC y RFID	13
2.2. RFID	15
2.2.1. Modos de operación	15
2.3. Ventajas y desventajas	16
2.3.1. Ventajas	16
2.3.2. Desventajas	17
2.3.3. Posibles amenazas y contramedidas en RFID	17
2.4. NFC	20

2.4.1.	Modos de operación de NFC	20
2.4.2.	Aplicaciones de NFC	21
2.5.	Ventajas y desventajas	21
2.5.1.	Ventajas	21
2.5.2.	Desventajas	22
2.5.3.	Posibles amenazas y contramedidas en NFC	22
3.	Estaciones de recarga del coche eléctrico (EVSE)	28
3.1.	Seguridad de los dispositivos EVSE desde un punto de vista ciberfísico	30
3.2.	Tipos de ataques centrados en dispositivos EVSE	33
3.2.1.	Ataques basados en la red	33
3.2.2.	Ataques físicos	35
3.2.3.	Ataques híbridos	36
3.3.	Enfoques para mejorar la seguridad CPS	36
3.3.1.	Seguro por diseño	37
3.3.2.	Seguridad del software	37
3.3.3.	Seguridad del hardware	38
3.3.4.	Supervisión y resistencia a la manipulación	38
3.4.	OCPP	38
4.	Arquitectura de un sistema basado en OCPP	42
4.1.	Protocolo OCPP 1.6	44
4.1.1.	Ejemplos de funcionamiento	44
4.1.2.	Modos de autorización local y funcionamiento sin conexión .	46
4.1.3.	Numeración de conectores	47
4.1.4.	Identificadores	47
4.1.5.	Identificadores superiores	48
4.1.6.	Operaciones iniciadas por el punto de recarga	49
4.1.6.1.	Authorize (autorizar)	49
4.1.6.2.	BootNotification (notificación de arranque)	50
4.1.6.3.	Heartbeat (latido)	51
4.1.6.4.	MeterValues (valores del medidor)	52
4.1.6.5.	StartTransaction (iniciar transacción)	54
4.1.6.6.	StatusNotification (notificación de estado)	55
4.1.6.7.	StopTransaction (detener transacción)	60
4.1.7.	Operaciones iniciadas por el CSMS	62
4.1.7.1.	ChangeConfiguration (cambiar configuración)	62
4.1.7.2.	ClearCache (limpiar caché)	63

4.1.7.3.	GetConfiguration (obtener configuración)	63
4.1.7.4.	RemoteStartTransaction (inicio de recarga remoto) .	64
4.1.7.5.	RemoteStopTransaction (detención de recarga remoto)	65
4.1.7.6.	Reset (reiniciar)	66
4.1.7.7.	UnlockConnector (desbloqueo de conector)	67
5. Gestión de proyecto software		68
5.1.	Alcance del proyecto	68
5.2.	Presupuesto	68
5.2.0.1.	Coste de personal	69
5.2.1.	Coste del hardware	69
5.2.2.	Coste total	70
5.3.	Plan de trabajo	70
5.3.1.	Identificación de tareas	70
5.3.2.	Estimación de tareas	71
5.3.3.	Planificación de tareas	73
5.4.	Gestión de recursos	74
5.4.1.	Especificación de recursos	74
5.5.	Gestión de riesgos	75
5.5.1.	Identificación de riesgos	75
5.5.2.	Análisis de riesgos	76
6. Solución		77
6.1.	Descripción de la solución	77
6.2.	El proceso de análisis y desarrollo	77
6.2.1.	Método basado en 2FA	78
6.2.2.	Método basado en NFC con etiqueta aleatoria	79
6.2.3.	Diseño	80
6.2.3.1.	Diseño de sistema	80
6.2.3.2.	Diseño detallado	82
6.2.4.	Implementación	90
6.2.5.	Pruebas	93
6.2.6.	Prueba de concepto	94
6.2.7.	Pruebas de posibles soluciones	107
6.2.7.1.	Autenticación 2FA	107
6.2.7.2.	Etiqueta NFC variable	110
6.2.7.3.	Combinación de autenticación 2FA y etiqueta NFC variable	111

7. Evaluación	112
7.1. Proceso de evaluación	112
7.1.1. Forma de evaluación	112
7.1.2. Casos de prueba	113
7.1.2.1. Autenticación 2FA	113
7.1.2.2. NFC variable	113
7.2. Análisis de resultados	113
Conclusiones	115
Lista de referencias	119
A. Control de versiones	123
B. Seguimiento de proyecto fin de máster	124
B.1. Forma de seguimiento	124
B.2. Planificación inicial	124
B.3. Planificación final	124

Índice de figuras

4.1.	Arquitectura del sistema propuesto	43
4.2.	Diagrama de secuencia de una recarga	45
4.3.	Diagrama de actualización de firmware	46
4.4.	Diagrama de <i>Authorize</i>	49
4.5.	Diagrama de <i>BootNotification</i>	50
4.6.	Diagrama de <i>Heartbeat</i>	51
4.7.	Diagrama de <i>MeterValues</i>	52
4.8.	Diagrama de <i>StartTransaction</i>	54
4.9.	Diagrama de <i>StatusNotification</i>	55
4.10.	Diagrama de <i>StopTransaction</i>	60
4.11.	Diagrama de <i>ChangeConfiguration</i>	62
4.12.	Diagrama de <i>ClearCache</i>	63
4.13.	Diagrama de <i>GetConfiguration</i>	63
4.14.	Diagrama de <i>RemoteStartTransaction</i>	64
4.15.	Diagrama de <i>RemoteStopTransaction</i>	65
4.16.	Diagrama de <i>Reset</i>	66
4.17.	Diagrama de <i>UnlockConnector</i>	67
5.1.	Diagrama de <i>Gantt</i> con la planificación de tareas	74
6.1.	Pantalla de login de la web	82
6.2.	Pantalla principal de la web	83
6.3.	Pantallas de usuario	84
6.4.	Pantallas referidas a puntos de recarga	85
6.5.	Pantallas referidas a las comunicaciones con los puntos de recarga . .	86
6.6.	Pantalla principal de login de la app	87
6.7.	Pantalla con el listado de cargas a confirmar	88
6.8.	Pantalla en la que introducir el código de confirmación de inicio de recarga	89

6.9. Diagrama de flujo del funcionamiento del protocolo OCPP 1.6 (izquierda) y añadiendo la autenticación 2FA (derecha) iniciando el proceso de recarga con una tarjeta	91
6.10. Diagrama de flujo del funcionamiento del protocolo OCPP 1.6 (izquierda) y añadiendo la autenticación 2FA (derecha) iniciando el proceso de recarga desde el CSMS	91
6.11. Diagrama de flujo del funcionamiento del protocolo OCPP 1.6 (izquierda) y añadiendo una etiqueta variable (derecha) finalizando el proceso de recarga con una tarjeta	93
6.12. Pantalla de <i>Mi Dispositivo</i>	95
6.13. Pantalla de <i>Opciones de desarrollador</i>	96
6.14. Pantalla de advertencia previa a desbloqueo de <i>Mi Unlock</i>	97
6.15. Pantalla de aviso de tiempo a esperar para desbloqueo de dispositivo mediante <i>Mi Unlock</i>	97
6.16. Pantalla de aviso de dispositivo correcto en <i>Mi Unlock</i>	98
6.17. Pantalla principal de TWRP	99
6.18. Proceso para formatear el dispositivo	100
6.19. Proceso para reiniciar en modo recovery	100
6.20. Proceso para instalar ficheros zip para rootear	101
6.21. Proceso para iniciar el móvil en funcionamiento normal	101
6.22. Pantalla de <i>Emulador de tarjetas Pro</i> tras instalar la app	102
6.23. Pantalla de <i>Emulador de tarjetas Pro</i> tras leer una tarjeta	103
6.24. Pantalla de <i>Emulador de tarjetas Pro</i> durante la emulación de una tarjeta	104
6.25. Pantalla de logs de <i>Ace Service Installer</i> tras el paso de tarjeta	105
6.26. Pantalla de logs de <i>Ace Service Installer</i> tras el paso del smartphone que simula la tarjeta	106
6.27. Pantalla de eventos de la web tras los pasos de las etiquetas	107
6.28. Pantalla del cargador en estado <i>Libre</i>	108
6.29. Pantalla del cargador tras enviar un <i>Authorize</i>	108
6.30. Ejemplo de correo electrónico que llega al usuario al solicitar un inicio de recarga	109
6.31. Pantalla del EVSE mientras se realiza una recarga	109
6.32. Pantalla del EVSE al pasar una tarjeta mientras se realiza una recarga	110
6.33. Pantalla del EVSE al pasar una tarjeta mientras se realiza una recarga	111
B.1. Diagrama de <i>Gantt</i> con la planificación final de tareas	125

Índice de tablas

4.1. Estados del punto de recarga y su tabla de flujo	55
4.2. Eventos que pueden llevar a cambios de estado	56
5.1. Presupuesto de personal	69
5.2. Presupuesto total	70
5.3. Estimación de tareas	73
B.1. Planificación final de tareas	125

Glosario de términos

Catálogo de términos específicos del contexto del trabajo.

ciberseguridad : Protección de los sistemas informáticos y de sus redes de comunicaciones, con el objetivo de mantener segura la información que procesan.

RFID : Radio Frequency Identification o identificación por radiofrecuencia. Es un sistema de almacenamiento y recuperación de datos remotos que usa dispositivos denominados etiquetas, tarjetas o transpondedores RFID.

NFC : Near-field communication o comunicación de campo cercano. Es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos.

IoT : Internet of Things o internet de las cosas. Describe objetos físicos (o grupos de estos) con sensores, capacidad de procesamiento, software y otras tecnologías que se conectan e intercambian datos con otros dispositivos y sistemas a través de internet u otras redes de comunicación.

UHF : Ultra High Frequency o frecuencia ultraalta.

HF : High Frequency o frecuencia alta.

LF : Low Frequency o frecuencia baja.

BAP : Battery-Assisted Pasive o pasivo asistido por batería son etiquetas RFID pasivas con una batería integrada.

EVSE : Electric Vehicle Supply Equipment o estación de carga eléctrica es un lugar que provee electricidad para la recarga rápida de las baterías de los vehículos eléctricos, incluyendo los vehículos híbridos enchufables.

EV : Electric Vehicle o vehículo eléctrico. Es un vehículo propulsado por uno o más motores eléctricos.

CPS : Cyber Physical System o sistema ciberfísico. Sistemas construidos mediante una integración segura y sin inconvenientes físicos y de computación.

AC : Alternating Current o corriente alterna.

DC : Direct Current o corriente continua.

OCPP : Open Charge Point Protocol o estándar de protocolo de punto de recarga abierto.

CSMS : Charging Station Management System o sistema de gestión de estaciones de carga. Es la designación del sistema de software backend al que se conectan todos los EVSE.

WS : WebSocket. Es una tecnología que proporciona un canal de comunicación bidireccional y full-duplex sobre un único socket TCP.

SOAP : Simple Object Access Protocol o protocolo simple de acceso a objetos.

JSON : JavaScript Object Notation o notación de objetos de JavaScript.

2FA : Two Factor Authentication o autenticación de doble factor. Trata de añadir un paso más a una autenticación simple (en el caso de este trabajo una tarjeta RFID).

Introducción

Actualmente, el cambio climático es un problema global. Por ello, gobiernos y otro tipo de entidades proponen reducir hasta la mínima expresión las emisiones de gases de efecto invernadero.

Uno de los principales causantes de la emisión de los gases de efecto invernadero es la automoción. Para ello, se cuenta con los vehículos eléctricos como una de las soluciones principales para reducir la emisión de este tipo de gases. Estos vehículos disponen de unos sistemas inteligentes de recarga a través de unos postes que se sitúan en domicilios particulares, comunidades de vecinos, en la calle, en electrolixeras...

Debido a la creciente producción y venta de este tipo de vehículos se está aumentando la producción e instalación de este tipo de estaciones de recarga. Todo ello aumenta los problemas de seguridad que se producen en torno a ellas. Tanto la seguridad como la privacidad de las personas que utilizan estos sistemas para recargar sus vehículos son necesarias para el despliegue exitoso de este tipo de tecnologías.

Los sistemas eléctricos, además, son cruciales para el desarrollo y la seguridad un país, siendo imprescindible un correcto funcionamiento de estos sistemas.

Estos sistemas tienen que cumplir los pretextos básicos de la ciberseguridad, a saber: confidencialidad, integridad y disponibilidad. Deben solo poder utilizar estos puntos los usuarios autorizados, recibiendo datos de pagos o recargas de la manera correcta siempre que quieran. Igualmente, el orden de prioridad de estos pretextos son en primer lugar la disponibilidad (es crucial el poder disponer de electricidad) y posteriormente la integridad y la confidencialidad (es mejor que un usuario vea sus datos comprometidos a que no se disponga de red eléctrica).

En resumen, el objetivo de este trabajo es el analizar el punto en el que se encuentra la seguridad y el desarrollo de este tipo de dispositivos, además de otros dispositivos que entran en juego en su funcionamiento en la parte de autorizar a los

usuarios correctos (tarjetas RFID o NFC). Además, se tratarán de diseñar algunas soluciones que reduzcan de forma poco costosa y sin afectar a estos puntos de recarga las posibles amenazas y vulnerabilidades de estos procedimientos de recarga de vehículos eléctricos.

Finalmente, no existe una única solución, estándar o mecanismo que pueda proporcionar todos los requisitos de seguridad necesarios para este tipo de estaciones de carga. Además, al haber un crecimiento y una mejora muy rápida de las tecnologías, estas soluciones tendrían que evolucionar con el paso del tiempo. Por otra parte, siempre es recomendable unir varias posibles soluciones para proporcionar la protección de seguridad general para sistemas tan complejo y mitigar los riesgos generales.

Metodología

En primer lugar para el correcto desarrollo del proyecto se han ido realizando reuniones semanales. Ello ha ayudado a tener un mejor seguimiento de las actuaciones que se iban realizando.

El trabajo propiamente dicho se ha realizado de la siguiente manera.

- En primer lugar se ha realizado un barrido de todos los campos que sirviesen para este trabajo. Es decir, se ha realizado un estado del arte, seleccionando los más interesantes para conocer la situación actual y decidiendo, con un conocimiento previo del tema a tratar, algunas de las posibles soluciones.
- En segundo lugar se ha realizado una prueba de concepto de explotación de una vulnerabilidad, a la vez que se iban decidiendo definitivamente estas posibles soluciones.
- Finalmente, se han desarrollado dos soluciones posibles para reducir la influencia de esta vulnerabilidad en la medida de la posible y se han realizado pruebas para comprobarlo.

Estructura del trabajo

Este trabajo dispone de nueve capítulos y un par de anexos de los que la descripción es la siguiente:

- Capítulo 1: se presenta el contexto en el que se realiza el trabajo. Se hace un estado del arte y se describe el problema.
- Capítulo 2: se describen las tecnologías RFID y NFC, su funcionamiento, sus diferencias y las vulnerabilidades.
- Capítulo 3: se trata la situación actual de la seguridad de estas estaciones de recarga y como se puede mejorar.
- Capítulo 4: se explica a grandes rasgos el funcionamiento del protocolo mediante el cuál operan estos puntos de recarga.
- Capítulo 5: se pretende realizar la gestión del proyecto, incluyendo la realización de los presupuestos, y gestión de tareas, recursos y riesgos.
- Capítulo 6: se realiza una prueba de concepto, y se proponen e implementan posibles soluciones para evitar la vulnerabilidad que explota la prueba de concepto.
- Capítulo 7: se analizan los resultados obtenidos con las pruebas tras la aplicación de las posibles soluciones.
- Capítulo 8: se expresan las conclusiones que se han obtenido en este trabajo.
- Anexo A: contiene la información sobre el control de versión utilizado para la realización el trabajo.
- Anexo B: trata el seguimiento del proyecto de fin de carrera.

Capítulo 1

Estudio del problema

En este capítulo el objetivo es presentar el contexto de realización del trabajo, realizando una revisión de las tecnologías, plataformas, herramientas o trabajos previos realizados en el mismo, llamado estado del arte.

1.1. El contexto del problema

Este proyecto se ha desarrollado en el Área de conocimiento de Arquitectura y Tecnología de Computadores de la Universidad de León. Las tecnologías tales como el punto de recarga, la manguera y el sistema CSMS han sido cedidos por la compañía Oxígeno Empresarial, S.L., en la que se disponen de diferentes sistemas para el desarrollo de aplicaciones de recarga de vehículos eléctricos.

1.2. El estado del arte

1.2.1. Metodología

1.2.1.1. Planificación de búsqueda

Para conocer el punto en el que se encuentran las investigaciones relacionadas con este trabajo que han sido realizadas anteriormente se realizará el estado del arte. La metodología de investigación se divide en las siguientes tres fases: planificación de búsqueda, proceso de búsqueda y selección de muestras, y extracción de datos y

preparación de informes. Para realizar el estudio seguimos las recomendaciones de Kitchenham [23], así como la guía PRISMA [24].

Tras comprobar que no se ha realizado un estudio centrado exactamente en el campo de interés de nuestro trabajo que responda a las preguntas planteadas en él, se ha procedido a la búsqueda de artículos de los que conforman el universo de estudio con el que se trabajará. Se ha considerado como fuente de información IEEE Digital Library.

1.2.1.2. Proceso de búsqueda

Una vez decididas las bases de datos en las que se van a realizar las búsquedas, es necesario construir cadenas de búsqueda adecuadas que permitan obtener resultados satisfactorios. Para la realización de la búsqueda se han construido varias cadenas que se aplican a cada una de las bases de datos indicadas anteriormente. Se utilizarán artículos de acceso libre.

La primera de ellas juntando a todas las tecnologías para conocer si hay alguna información combinada de ambas

SS1('charging station' AND 'vehicle' AND ('security' OR 'cybersecurity') AND ('RFID' OR 'NFC'))

Mediante esta cadena de búsqueda se intentó recopilar un conjunto de artículos en los que se encuentren todos los términos del trabajo. Uno de los filtros que se aplican durante la búsqueda es el relacionado con la fecha de publicación del artículo. Al ser campos tecnológicos, con cambios muy veloces, como es la ciberseguridad, nos centraremos únicamente en artículos recientes. En este caso, la búsqueda se centra en artículos publicados entre el año 2019 a hoy. En esta búsqueda se obtuvieron 2 artículos, recogiendo ambos.

Al tratarse de poca información, se decide ampliar la búsqueda y separarlo en dos búsquedas. Se realiza de este modo para conocer el estado de ambas tecnologías por separado.

SS2(('security' OR 'cybersecurity') AND ('RFID' OR 'NFC')) SS3('charging station' AND 'vehicle' AND 'security')

Con la primera de las búsquedas se pretenden encontrar, además de datos de los posibles ataques y vulnerabilidades de ambas tecnologías, algún procedimiento

que reduzca las que se relacionan con el problema que se trata en este trabajo para poder adaptarlo o recoger alguna idea relacionada con los mismos.

En la segunda de las búsquedas el objetivo es más simple, basado en entender mejor la tecnología de los puntos de recarga del coche eléctrico y en algunos procedimientos para complementar y mejorar y completar las medidas de seguridad aplicadas en relación a las tecnologías RFID/NFC y al propio entorno de funcionamiento del punto de recarga.

En este caso el tiempo de búsqueda es menor, ya que hay un mayor número de artículos y, como se ha mencionado anteriormente, las tecnologías NFC y los cargadores de coche eléctrico tienen una evolución muy rápida y constante. Por ello y, tras filtrar la búsqueda por año de publicación a partir del año 2021 hasta la actualidad, se obtuvieron en la primera de las búsquedas 233 resultados, mientras que en la segunda búsqueda 83 resultados.

1.2.1.3. Selección de muestras

Para seleccionar las muestras obtenidas se va a realizar un proceso de filtrado. Se realiza en primer lugar un filtrado en base a la lectura del título y del resumen de cada uno de los artículos. Para decidir si un determinado artículo se marca como aceptado o rechazado, se han establecido una serie de criterios. En caso de que un artículo comparta un criterio de exclusión y un criterio de inclusión se le dará más peso al criterio de exclusión. Así se tratará de eliminar aquellos artículos que cumplan al menos un criterio de exclusión o que no cumplan alguno de los criterios de inclusión. Igualmente, se volverá a revisar el resumen al final para realizar un nuevo filtrado en caso de que quede un gran número de artículos.

Los criterios de inclusión establecidos son los siguientes:

- CI1 El artículo hace algún tipo de revisión de la tecnología a utilizar.
- CI2 El artículo trata sobre alguna posible vulnerabilidad.
- CI3 El artículo propone algún método para reducir las vulnerabilidades.

Los criterios de exclusión establecidos son los siguientes:

- CE1 El artículo no pertenece al ámbito de la ciberseguridad.
- CE2 El artículo es una revisión de la literatura.
- CE3 El artículo no es de libre acceso.

- CE4 El artículo no está en inglés ni en español.

Para conocer qué cantidad de artículos se deben analizar y qué puntos son los más interesantes a recoger para este trabajo se ha desarrollado un cuestionario de evaluación de la calidad del artículo, en base a ciertos requisitos que son de interés en esta investigación. Este cuestionario se ha realizado a partir de la información obtenida tras la lectura completa de los artículos que se han seleccionado en la fase anterior. El cuestionario que permitirá evaluar los artículos antes de pasar a la extracción de resultados está compuesto por las siguientes preguntas:

- P1 ¿Trata el diseño de un método de seguridad?
- P2 ¿Reduce la influencia de una vulnerabilidad concreta?
- P3 ¿Trata algunos desafíos en materia de seguridad informática?
- P4 ¿Trata de forma global de alguna de las tecnologías de las que se pretende hablar en este trabajo?

Las preguntas indicadas han sido escogidas en base a las características de un artículo que tiene mayor interés para la investigación, es decir, en este estudio se trata de obtener la situación actual en la ciberseguridad de las tecnologías NFC y de los puntos de recarga de coche eléctrico, además de métodos que traten de enfrentarse a algunas de las vulnerabilidades actuales.

Una vez elegidas las preguntas, es necesario establecer cuáles son las posibles respuestas a las preguntas antes mencionadas y qué valor tendrá cada una de las respuestas. Para la construcción de este cuestionario se ha tratado de formular todas las preguntas de manera que pudieran tener una respuesta del tipo Sí, o No, otorgando a estas respuestas 1 punto y 0 puntos, respectivamente. De esta forma, la valoración máxima que puede alcanzar un artículo es de tres puntos. En este sentido, se ha establecido un umbral en dos puntos, incluyendo únicamente los artículos con una puntuación de 2 o 3, con el objetivo de que los artículos sean lo más completos posible.

1.2.1.4. Extracción de datos

Como último paso en la metodología propuesta, es necesario establecer el método de extracción de los datos que son de interés para la investigación. Una vez reducido el universo de estudio en los artículos que se ajustan a la investigación que se desea realizar, se ha establecido un formulario de extracción de datos. Las variables que se

extraerán de cada uno de los artículos se han obtenido de las preguntas de investigación indicadas en el capítulo de este artículo que sirve de introducción. Los datos se extraerán de la lectura completa y detallada de cada uno de los artículos. Las variables que se desean obtener de cada artículo se han establecido respetando el objetivo de realizar una revisión sistemática y por tanto preservando la posibilidad de que esta extracción sea replicable y objetiva. De esta forma las variables que se extraerán, si procede, son las siguientes:

- D1 Tipo y nombre de diseño
- D2 Vulnerabilidad que reduce
- D3 Desafíos en materia de ciberseguridad en los que influye
- D4 Tecnología sobre la que presenta alguna visión global

1.2.2. Resultados

Finalmente, el número de artículos se ha reducido a catorce. Se ha podido cubrir de forma global todas las cuestiones y se proceden a comentar estos resultados

Para las tecnologías NFC y RFID se han recogido los siguientes artículos:

- En [1] se propone un algoritmo de encriptación ligero llamado “SWLEA”, en el que la longitud del bloque de datos del algoritmo es de 32 bits y admite claves de 32 bits, aplicándose principalmente al sistema con chip de etiqueta RFID como chip identificador.
- En [2] se diseña una metodología para una comunicación eficiente entre dispositivos NFC activos que utilizan el modo de lectura/escritura NFC, diseñando un sistema seguro de autenticación multifactor (MFA) que requiere comunicación bidireccional para la autenticación mutua de dos dispositivos NFC, verificándose experimentalmente utilizando teléfonos inteligentes *Android* habilitados para NFC y un servidor *Kerberos* como autenticador de terceros.
- En [3] se propone un esquema de autenticación RFID eficiente (RFID-AS) basado en Signcryption de curva hiperelíptica, el cual proporciona las funciones de seguridad necesarias para el sistema RFID, así como la seguridad frente a posibles ataques.
- En [4] se propone un nuevo mecanismo de seguridad consistente en un protocolo ligero de autenticación mutua y un diseño de etiqueta antifalsificación,

basado en combinar el esquema de encriptación de clave pública de *Rabin* con la tecnología de funciones físicamente no clonables (PUF).

- En [5] se presenta el diseño y la implementación de Au-Hota, un sistema que puede autenticar la etiqueta y el usuario simultáneamente, y puede resistir el ataque de reproducción y el ataque de suplantación que no pueden resolverse con la mayoría de los métodos de capa física, asignando un identificador único al usuario basado en el acoplamiento inductivo entre dos etiquetas adyacentes.
- En [6] se propone un nuevo mecanismo de autenticación ligero basado en *sponge permutation* sin servidor para probar la autenticidad de las etiquetas RFID a cualquier lector legítimo y viceversa.
- En [7] se presenta un esquema de diseño que combina tecnología embebida con tecnología biométrica para implementar un sistema de control de acceso RFID basado en Raspberry PI.
- En [8] se diseña una función de encriptación ultraligera y se propone un esquema de autenticación RFID basado en esta función para el entorno colaborativo de extremo a extremo en la nube.

Los siguientes artículos han sido seleccionados para el sistema de recarga de vehículos eléctricos:

- En [9] se estudia el panorama actual de las estaciones de carga de vehículos eléctricos en términos de seguridad cibernética, se identifican las vulnerabilidades cibernéticas y se presentan protocolos y estándares que puedan abordar los desafíos de seguridad cibernética en dichos sistemas para proporcionar una infraestructura de carga más segura, además de recomendar el uso de algunas medidas y técnicas de seguridad para mitigar los ataques cibernéticos en la infraestructura de carga de vehículos eléctricos y aliviar el impacto adverso de tales ataques.
- En [10] se presentan las entidades que participan en un escenario de carga inteligente basado en OCPP, se identifican problemas y amenazas de seguridad y se presentan soluciones propuestas por académicos, además de problemas de seguridad abiertos para OCPP para los que se proponen direcciones de investigación futuras para la mejora de la seguridad del protocolo.
- En [11] se tratan los desafíos en materia de ciberseguridad en la infraestructura del vehículo eléctrico

- En [12] se proporcionan un conjunto de protocolos de autenticación livianos que permiten la autenticación mutua y el acuerdo de clave de sesión entre el vehículo eléctrico y el sistema de carga, al tiempo que brinda protección contra numerosos ataques.
- En [13] el esquema propuesto implementa un mecanismo de seguridad basado en las características inherentemente únicas de la biometría del ojo humano, que se trata de una autenticación eficiente y de bajo coste, utilizando k-Nearest Neighbors (KNN), que es un algoritmo de cifrado liviano.
- En [14] se propone un mecanismo de autenticación robusto para cargar vehículos eléctricos.

Con ello ya se dispone de la información suficiente para poder encontrar algunas soluciones a los problemas de seguridad que presentan este tipo de tecnologías, teniendo un punto de partida con una importante base de posibilidades y datos de las mismas.

1.3. Definición del proyecto

1.4. La definición del problema

Los equipos de suministro de vehículos eléctricos (EVSE), también conocidos como estaciones de recarga, sirven para cargar los vehículos eléctricos. Los EVSE contienen sistemas de computación conectados a Internet. Estos sistemas cumplen importantes funciones de control, tales como la autorización, la recarga de vehículos eléctricos y la conexión a la red eléctrica local. Las estaciones de carga autorizan a usuarios y vehículos mediante tarjetas RFID o NFC, Bluetooth o Wi-Fi.

Por todo ello, hay muchos componentes de detección, comunicación y computación en los EVSE que son potencialmente vulnerables a los ataques de ciberseguridad. Como en todos los ataques, los piratas informáticos tratan de explotar estas vulnerabilidades para comprometer la disponibilidad, la integridad y la confidencialidad de la red. En este caso, se habla de una red de estaciones de carga o incluso la red eléctrica. Dado el tremendo crecimiento del mercado de vehículos eléctricos en los próximos años, es importante diseñar estaciones de carga confiables. El diseño de estaciones de carga confiables necesita una comprensión más profunda de las

interacciones ciberfísicas dentro de la estación de carga, así como de las relaciones entre los componentes cibernéticos y físicos.

Se presenta un enfoque de sistema para comprender los posibles ataques a este tipo de sistemas. Además se tratará el estado de los sistemas de carga inteligente y de los sistemas de comunicaciones NFC. Se propone una estructura de sistema basica para dirimir las autorizaciones para poder recargar basada en un servidor web y una base de datos. Finalmente se propondrá un sistema conceptual para evitar los ataques de acceso no autorizado a nivel físico al punto de recarga (robo de datos NFC o denegación de servicio (DoS) para mejorar la seguridad de estos sistemas.

Capítulo 2

Tecnologías NFC y RFID

NFC significa Near Field Communication, comunicación de campo cercano. Es una plataforma abierta de comunicación pensada para enviar datos de un dispositivo a otro, pensada desde un inicio para sistemas móviles. Utiliza esquemas básicos de comunicación de identificación por radiofrecuencia (RFID). Opera en una frecuencia de 13,56 MHz con una tasa de datos de hasta 424 kilobits por segundo a una distancia de 10 centímetros [15]. Tiene además la posibilidad de tener una comunicación bidireccional o en modo P2P (peer-to-peer).

Esta tecnología es una extensión de RFID. Ambas funcionan a la misma frecuencia. NFC es una RFID muy similar, pero existen algunas diferencias entre estas tecnologías, como la distancia de escaneo y las formas de comunicación.

Los dispositivos habilitados para NFC pueden comunicarse entre sí cuando se encuentran dentro del rango operativo antes mencionado. La tecnología NFC ha sido la fuente de muchas implementaciones en varios negocios, por ejemplo en los sistemas de control de acceso, identificación personal o de activos, pagos... todo ello mediante el uso de tarjetas de identidad, pasaportes o algunos dispositivos móviles.

NFC tiene tres modos de funcionamiento de dispositivo típicos: modo de emulación de tarjeta, modo de lector/grabador y modo de igual a igual [17]. Este modelo involucra dos dispositivos para la comunicación, uno que la inicia y otro que funciona a modo de objetivo. El dispositivo iniciador inicia la comunicación siendo este habitualmente un dispositivo NFC activo. El iniciador es el dispositivo responsable de dar energía al dispositivo objetivo en caso de que este último sea un dispositivo pasivo, ya que el primero posee un componente de energía que también puede generarla para el objetivo. El dispositivo de destino puede ser una etiqueta RFID, o un

dispositivo o una tarjeta basada en ello. Los dispositivos de destino responden a las solicitudes.

La comunicación entre los dispositivos se realiza a través de una única banda de RF compartida por los dispositivos en modo semidúplex [18]. Un dispositivo transmite en un momento y el otro dispositivo está en modo de escucha. El segundo dispositivo inicia su transmisión una vez que el primer dispositivo la ha finalizado. Los dispositivos móviles basados en NFC, habitualmente smartphones (teléfonos inteligentes), se pueden usar tanto en el modo iniciador como objetivo simultáneamente mediante el uso sencillo de la interfaz disponible en la pantalla del propio smartphone. Las aplicaciones desarrolladas para ellos tienen una gran variedad de usos de esta tecnología NFC, como por ejemplo identificación o operaciones bancarias.

Los dispositivos NFC deben cumplir con las normas ISO/IEC 18092 e ISO/IEC 14443. El primero define los modos de comunicación para la interfaz y el protocolo de comunicación de campo cercano y el otro es para tarjetas de identificación u objetos de intercambio internacional.

Esta tecnología es una de las más importantes de IoT, ya que permite una interconexión fácil y segura entre objetos. IoT es una agrupación e interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet), donde todos ellos podrían ser visibles e interactuar entre sí. Todo lo que se necesitaría para utilizarla en los smartphones más modernos es encender la conectividad NFC del mismo y escanearlo en un lector de dispositivo.

Por otro lado, RFID , es igualmente tecnología inalámbrica como NFC. En este caso se utiliza, a menudo, en tarjetas o etiquetas de acceso. Tiene dos componentes: etiquetas y lectores. El lector es un dispositivo con antenas. Emite ondas de radio y recibe señales de la etiqueta RFID. Cuando el lector reconozca la etiqueta, confirmará la identidad y le dará acceso.

Si bien estas dos tecnologías tienen casi la misma funcionalidad, y para el uso del trabajo que se describirá más adelante la misma, son diferentes.

2.1. Diferencias entre NFC y RFID

Son varias las diferencias existentes entre ambas tecnologías. Sin embargo, se pueden considerar a los sistemas NFC como un subgrupo de la tecnología RFID, siendo en realidad parte de estas tecnologías RFID.

La diferencia más importante es que los componentes RFID pueden operar y comunicarse entre sí a una distancia mayor que los NFC. Aunque ambos procesos se pueden utilizar para transmitir datos de forma remota, RFID en su conjunto se refiere a la tecnología de identificación inalámbrica por radiofrecuencia. En cambio, los dispositivos NFC están dedicados a la comunicación inalámbrica de corto alcance mediante tarjetas de proximidad. A diferencia de NFC, la etiqueta RFID, se puede escanear a una distancia de hasta 100 centímetros [16]. EN el caso de RFID solo hay comunicación unidireccional que opera solo activa (de 0 a 10 centímetros de distancia) y pasiva (de 10 a 100 centímetros de distancia).

Por otro lado, los sistemas RFID son muy útiles en los entornos industriales para recoger información, entre otras cosas, de paquetes e inventarios, recopilando estadísticas e información relevante sobre los objetos. También se utilizan en el cronometraje de carreras y en algunos eventos para control de acceso y seguimiento de los asistentes. Además, también se emplean por ejemplo en tiendas de ropa para identificar las prendas y su ubicación, estableciendo una medida extra de seguridad. Sin embargo, las etiquetas NFC se utilizan en tan habituales como los teléfonos móviles y las tarjetas bancarias *contactless*, con las que se paga en los TPV de los comercios. Algo similar puede ocurrir con las tarjetas que permiten la entrada de las personas autorizadas a los edificios mediante sistemas de control de acceso y también para abrir cerraduras electrónicas de hoteles y alojamientos similares.

Una de las características fundamentales de NFC es la comunicación entre pares. Un dispositivo NFC puede actuar tanto como lector como etiqueta. Eso significa que puede transferir y recibir datos de otro dispositivo que también sea NFC. Simplemente se necesitan tener los dos dispositivos juntos. Por ejemplo, pueden convertirse en dispositivos para compartir datos. Al final de esta comunicación, ambos teléfonos tendrán la misma copia de la información. Sin embargo, RFID solo puede leer datos e interpretarlos. Por ejemplo, el recorrido de un paquete en una planta industrial. Esto se puede conocer viendo a qué horas y a qué lectores se acercó el paquete con la etiqueta RFID, conociendo su comportamiento. Pero, por tanto, no puede transferir o extraer estos datos a otro dispositivo RFID.

2.2. RFID

2.2.1. Modos de operación

Hay varios tipos de funcionamiento de las etiquetas RFID dependiendo de cómo la etiqueta se comunica con el lector. Estos modos son pasivo, activo y semipasivo (pasivo asistido por batería).

1. Activo:

Las etiquetas RFID activas tienen tanto su propio transmisor como una fuente de energía (batería) en la etiqueta. Estas son, en su mayoría, soluciones UHF, y los rangos de lectura de las mismas pueden extenderse hasta los 100 m en algunos casos. Las etiquetas activas suelen ser más grandes y caras que las pasivas, y se utilizan para rastrear grandes activos (como contenedores de carga, vehículos y máquinas). Además también suelen estar equipadas con sensores que miden y transmiten datos de temperatura, humedad, luz y golpes y vibraciones de los objetos a los que se pegan.

Hay dos tipos de etiquetas activas. Por un lado los transpondedores, los cuales solo se "despiertan" y transmiten datos cuando reciben una señal de radio de un lector. Por ejemplo, al conectar uno de estos dispositivos a un vehículo destinado al pago en telepeajes o al paso por puntos de control este solo se activaría si pasase por un paso o puerta en particular. Esto es algo que ayuda a conservar la vida de la batería. Por otro lado están las balizas, las cuales emiten una señal en un intervalo preestablecido. Este tipo de etiqueta activa se utiliza en los sistemas de ubicación en tiempo real (RTLS), utilizados para rastrear cualquier cosa, desde contenedores de carga preparados para enviarse en un barco o en dispositivos sanitarios como camas o sillas de ruedas.

2. Pasivo:

En las soluciones basadas en etiquetas RFID pasivas, tanto el lector como su antena envían una señal a la etiqueta, la cual se utiliza para encender la etiqueta y reflejar la energía de regreso al lector. Hay sistemas pasivos de LF, HF y UHF. En este caso los rangos de lectura son más reducidos que los de las etiquetas activas y están limitados por la potencia de la señal que se refleja en el lector (se conoce como retrodispersión de etiquetas).

Habitualmente las etiquetas pasivas son más pequeñas, menos costosas y más flexibles que las activas. Esto significa que se pueden adjuntar o incluso incrustar.

tar en una mayor variedad de objetos. Las etiquetas UHF pasivas se utilizan habitualmente, por ejemplo, para el seguimiento a nivel de artículo de algún tipo de bien de consumo y productos farmacéuticos.

3. Semipasivo (BAP):

También existe un tercer tipo híbrido de etiqueta RFID. Los sistemas BAP o sistemas RFID semipasivos incorporan una fuente de alimentación en una configuración de etiqueta pasiva. La fuente de alimentación ayuda a garantizar que toda la energía recogida del lector se pueda utilizar para reflejar la señal, lo que hará que mejoren tanto la distancia de lectura como las tasas de transferencia de datos. A diferencia de los activos, estas etiquetas BAP no tienen sus propios transmisores

2.3. Ventajas y desventajas

2.3.1. Ventajas

- RFID ofrece una forma rápida y confiable de rastrear activos. Se puede aplicar a varios componentes en una línea de producción. Puede usarse para rastrear equipos o contenedores de alto valor que necesitan tener algún tipo de seguimiento.
- Se puede utilizar RFID para instalar lectores fijos en puntos clave. Elimina la necesidad de presentar algún tipo de identificación manualmente. En una línea de producción eliminaría la necesidad de intervención manual. RFID promueve la eficiencia y la precisión.
- RFID mejora la salud y la seguridad. Las empresas pueden usarlo para rastrear qué activos necesitan una inspección. También pueden usarlo para restringir el acceso a estos activos cuando no se cumplen estas condiciones de acceso. RFID agiliza las inspecciones y la generación de informes.
- La tecnología RFID se puede integrar con otras tecnologías. Se puede integrar con la automatización de entregas y sistemas de elección de stocks, ahorrando tiempo desde el pedido hasta el envío de artículos.
- La mejora de todo esto mediante RFID provoca un aumento de los ingresos en una empresa que lo implemente dado que mejora la gestión y la organización. Con ello, se aumenta la satisfacción de los clientes, lo que hace que una empresa

sea más competitiva. Esto, lógicamente, produce mayores ventas y mejores márgenes.

2.3.2. Desventajas

- El coste de RFID puede ser diez veces más que algunos sistemas anteriores, como el código de barras, lo que evita que algunas empresas o sistemas eviten su uso (por ejemplo, el acceso a algunos eventos).
- En el caso de las tarjetas de acceso, estas deben ser tenidas en cuenta para su uso. Sin embargo, no hay capacidad de seguimiento en caso de que se pierdan. Las tarjetas de acceso extraviadas son una pérdida para las empresas, organizadores de eventos... y un riesgo de seguridad para los mismos. El usuario final también debe averiguar cómo acceder en caso de que pierda su tarjeta de acceso.
- Otra desventaja es que RFID no puede funcionar cuando no hay energía. Algunas empresas con generadores aún pueden utilizar sistemas RFID en estos casos (por ejemplo, el acceso a alguna sala de hospitales), pero otras que no lo tienen pueden necesitar cambiar al bloqueo manual o permitir el acceso libre eventualmente hasta que se recupere la energía, con el riesgo de seguridad que eso conlleva.

2.3.3. Posibles amenazas y contramedidas en RFID

Existen numerosas formas de atacar a los clientes que utilizan la tecnología RFID tanto a su privacidad y seguridad física como a su privacidad informativa y sus autorizaciones públicas.

La tecnología RFID comprende preocupaciones crecientes de seguridad y privacidad. Todo ello es basado en que en el proceso de radiación de radiofrecuencia que se utiliza para leer etiquetas RFID no intervienen los seres humanos y en que estas etiquetas RFID no son capaces de mantener el historial de lecturas pasadas. Además, estas etiquetas son legibles sin el conocimiento del propietario.

Los ataques que mayormente ocurren son los siguientes.

- Ataque de análisis de energía:

Un ataque de análisis de energía se utiliza para robar información y obtener

acceso a una red. Estos ataques se pueden montar en los sistemas RFID para la observación del nivel de consumo de energía de una etiqueta.

Se basan en las propiedades físicas básicas del dispositivo, los cuales se rigen por las leyes de la física. Estas dictan que las variaciones de voltaje dentro del dispositivo se producen debido a movimientos muy pequeños de cargas eléctricas (corrientes). Al medir esas corrientes es posible aprender cierta cantidad de información sobre los datos que se manipulan.

- *Eavesdropping* (escucha a escondidas):

Este ataque se produce cuando un lector RFID no deseado intercepta una conversación entre un lector y una etiqueta y, gracias a ello, obtiene información. Para los atacantes es necesario tener un buen conocimiento sobre los protocolos específicos de RFID, la etiqueta que se utiliza en la comunicación etiqueta y la información del lector. Este ataque se utiliza tanto para robar información como para obtener acceso.

Para reducir las posibilidades de un ataque de este equipo se recomienda el no utilizar siempre estas etiquetas RFID en caso de datos críticos y el uso de técnicas de encriptación y algún tipo de blindaje.

- Ataque de reproducción:

Se basa en escuchar a escondidas y atacar cuando una parte de la conservación finaliza en los sistemas RFID, retransmitiéndola a partir de ahí varias veces, pudiendo con ello interceptar la comunicación de los sistemas RFID.

Para tratar de reducir este tipo de ataques se pueden ir eliminando progresivamente etiquetas (incorporando otras nuevas), bloqueando accesos cuando hay sospechas de posible robo de claves de acceso y usando sedónimos para reducir el robo de información o utilizar algún tipo de técnica de encriptación. Además se pueden reducir las posibilidades de escucha utilizando protocolos de límite de distancia o reduciendo la intensidad de la señal.

- Ataque de clonación:

Se basa en reproducir información de una etiqueta/sensor preexistente. Los atacantes pueden clonar cualquier etiqueta o sensor auténtico si cuentan con el equipo adecuado para hacerlo. Tras ello se podrán comunicar con un lector auténtico. El sensor o la etiqueta clonados afirman ser los genuinos y el lector estará dispuesto a aceptarlo, siendo esta falsa.

Igual que en el caso anterior, hay opciones para reducir estos ataques basándose en la eliminación de etiquetas y sustitución de estas mismas por otras cada cierto tiempo, también bloqueando accesos cuando hay sospechas de posible robo de claves de acceso y utilizando sedónimos para reducir el robo de información o encriptando los datos de estas tarjetas. Y, como ya se vio, se podrían reducir las posibilidades de escucha utilizando protocolos de límite de distancia o reduciendo la intensidad de la señal.

- Ataque de suplantación de identidad:

Cuando un atacante logra con éxito sus objetivos en un ataque de clonación, donde el atacante puede registrar o leer la información entre la etiqueta y el lector. Luego, el atacante emula esta información y la vuelve a transmitir al lector, apareciendo esta información en el lado del propio lector como etiqueta válida.

Dado que son casos similares que los anteriores se utilizarán las mismas estrategias para la defensa contra estos ataques, como la eliminación de etiquetas y sustitución de estas mismas por otras cada cierto tiempo, el bloqueo de los accesos en el momento en el que haya sospechas de posible robo de claves de acceso y la utilización de sedónimos para reducir el robo de información o la encriptación los datos de estas tarjetas. También como en los casos anteriores se pueden reducir las posibilidades de escucha utilizando protocolos de límite de distancia o reduciendo la intensidad de la señal.

- Ataque de denegación de servicio (DoS):

Se suele realizar ejecutando varias peticiones, en este caso comunicaciones RFID, para desbordar al lector y evitar que los usuarios legítimos puedan acceder. La interferencia de la señal en el canal radiofrecuencia es un ejemplo común de un ataque DoS para los sistemas RFID. Este ataque trata con datos de etiquetas y tiene lugar cuando un atacante niega el servicio de un usuario válido.

Se pueden utilizar para evitarlo algún mecanismo de control, firewall o con protocolos más eficientes.

- Ataque físico:

En los ataques físicos, el atacante manipula las etiquetas físicamente, en ocasiones utilizando laboratorios para ello. Las etiquetas RFID suelen ofrecer una resiliencia mínima o incluso nula contra los ataques físicos.

- Modificación de datos físicos:

En este caso el atacante trata de alterar los datos almacenados en la memoria de etiquetas RFID.

Se pueden tratar de evitar estos ataques tanto protegiendo la memoria de estos dispositivos como utilizando protocolos criptográficos seguros.

- Inyección de información:

En este caso el atacante trata de introducir en la comunicación algún dato sobrante para evitar el acceso del cliente.

Este ataque se puede evitar chequeando la información que se envía y recibe cada cierto tiempo.

2.4. NFC

2.4.1. Modos de operación de NFC

1. Emulación de tarjeta:

Los dispositivos de los smartphones actúan como una smartcard sin contacto cuando se usan en el modo de emulación de tarjeta, utilizándose por ejemplo en sistemas de pago y emisión de entrada. Las aplicaciones de los smartphones utilizan bibliotecas de la infraestructura existente de smartcards (tarjetas inteligentes). Estos dispositivos móviles se pueden usar en lugar de las smartcards que se usan para pagos o control de acceso físico, etc. El controlador NFC actúa como una puerta de enlace para dirigir los datos y comandos desde la aplicación de la tarjeta en el smartphone hasta el hardware receptor. El controlador NFC en sí mismo no realiza ningún cálculo. Esta implementación ahora se conoce como emulación de tarjeta basada en host, generando respuesta el sistema operativo al tráfico NFC recibido de lectores externos.

2. Lector/grabador:

Permite que los smartphones lean datos de dispositivos NFC o tarjetas inteligentes que contienen etiquetas RFID. También se pueden usar en el modo de escritura donde se usa para escribir datos de información de etiquetas en las etiquetas en blanco y no inicializadas. Un dispositivo inteligente habilitado para NFC puede leer etiquetas NFC. Un usuario puede recuperar la información de los datos almacenados en la etiqueta para otras acciones posteriores.

3. Igual a igual:

Dos dispositivos pueden actuar como dispositivo activo y pasivo. La comunicación bidireccional tiene lugar entre dos teléfonos móviles habilitados para NFC para intercambiar información. La comunicación entre se realiza en modos semidúplex por el mismo canal. El formato de intercambio de datos NFC o NDEF [19] es un formato estandarizado que se utiliza para almacenar datos en etiquetas. También especifica los estándares para el transporte de datos entre dos dispositivos NFC en modo P2P (Peer-to-Peer) [20].

2.4.2. Aplicaciones de NFC

La clasificación de las aplicaciones NFC depende del comportamiento de la comunicación. Se puede dividir en cuatro tipos.

1. *Touch and go*: Requiere que el consumidor acerque o toque con el dispositivo NFC al lector NFC para que las tareas se ejecuten en la aplicación.
2. *Touch and confirm*: Requiere que el consumidor confirme la interacción aceptando la transacción de pago o ingresando una contraseña para la confirmación del sistema.
3. *Touch and connect*: Conectarse para habilitar la transferencia de datos punto a punto entre dos dispositivos habilitados para NFC.
4. *Touch and explore*: El consumidor podrá encontrar y explorar aplicaciones y funcionalidades del sistema.

2.5. Ventajas y desventajas

2.5.1. Ventajas

- NFC simplifica los procesos de pago. Con un teléfono inteligente o una tablet, los clientes pueden pagar fácilmente al finalizar una compra. Los clientes pueden usar una billetera móvil como las que ofrecen Google o Apple. Con solo unas pocas órdenes se pueden realizar transacciones. Dado que no es necesario llevar dinero en efectivo, protege contra algunos tipos de robos a la fuerza.
- NFC usa códigos pin. En el peor de los casos los ladrones pueden robar el teléfono pero no el dinero. Sin un código especial como el pin no pueden ni

obtener ni transferir el dinero, por ello a los clientes también les pueden dar una mayor confianza las empresas que permiten este tipo de pagos inteligentes.

- Los pagos con NFC son más seguros que el uso de la banda magnética de una tarjeta de crédito. El primero tiene una seguridad más estricta, por lo que los clientes pueden estar seguros de que sus transacciones de dinero están seguras, además de sus datos personales.
- NFC es versátil, cubriendo una amplia gama de servicios. Las empresas lo utilizan para la implementación de plataformas de pago, banca móvil y reservas en eventos u hostelería, o billetes de tren. También se puede utilizar para entregar actualizaciones de algunos datos (por ejemplo, presencia) en tiempo real.

2.5.2. Desventajas

- Estas tecnologías NFC podrían ser excesivamente caras para algunas empresas, dado que requiere el uso de un conjunto de dispositivos y equipos que pueden elevarse en coste, además de incluir también estándares que dependen de la actualización. Algunos grandes minoristas han incorporado ya estos sistemas para su proceso de pago. Por el contrario, algunas pequeñas tiendas todavía los pueden encontrar demasiado caros. Además, el coste de contratar técnicos e instaladores de software puede aumentar rápidamente, por lo que este tipo de empresas deben buscar otras formas de prepararse para la aplicación de NFC.

2.5.3. Posibles amenazas y contramedidas en NFC

1. Ataques que afectan a la confidencialidad:

a) *Eavesdropping* (escucha a escondidas):

La comunicación NFC se lleva a cabo en modo inalámbrico, algo que siempre aumenta las posibilidades de espionaje en las comunicaciones. Es una amenaza muy importante en este tipo de comunicaciones, implicando el uso de recursos adicionales para frenar este tipo de ataques. La comunicación entre dos dispositivos a través del canal NFC puede ser interceptada o recibida por un atacante que se encuentre con proximidad geográfica

a estos dispositivos. El atacante podría utilizar antenas receptoras más potentes y grandes que las de los dispositivos móviles para recibir la comunicación, lo que facilita que estas escuchas se puedan realizar a grandes distancias, mayores a los 10 centímetros para la comunicación de este tipo de dispositivos.

La tecnología NFC no tiene ninguna protección específica o particular contra esta posibilidad. Aunque la transmisión de datos en modo pasivo es más difícil de atacar que en modo activo, no se puede recurrir únicamente al uso del modo pasivo, ya que muchas aplicaciones actualmente transmiten los datos en modo activo.

La única solución a este tipo de vulnerabilidad es utilizar un canal seguro, basando la comunicación a través del canal NFC con un tipo de autenticación que utilice esquemas de autenticación y cifrado.

b) Ataque de confianza:

Este ataque explota el cumplimiento del protocolo de NFC. Lo que realiza el atacante es intentar robar la información de la tarjeta de la víctima haciéndose pasar por el propietario de la misma. El sistema de acceso de la víctima no podrá revelar el ataque porque pensará que hay una tarjeta frente a él. Al tratarse de un protocolo sin contacto, el atacante necesita una distancia corta.

Hay varias formas posibles para protegerse del ataque de retransmisión. Una de estas formas mediante el uso de un contenedor hecho de algún material que sea impenetrable a través de señales de radio (*Jaula de Faraday*).

Otra forma es usar el protocolo de límite de distancia, basado en la adición de un límite de seguridad adicional al sistema.

Hay una tercera manera, que es una protección perfecta, basada el uso de un canal seguro igual que en el caso de *Eavesdropping*.

c) Lectura de larga distancia:

Se basa en una modificación del dispositivo NFC. Lo que hace es aumentar el alcance de la alta frecuencia, por lo que el atacante podría leer las etiquetas desde una distancia segura.

2. Ataques que afectan a la integridad:

a) Corrupción de datos:

Los datos transmitidos a través de la interfaz NFC pueden ser modificados por un atacante si consigue interceptarlos. La corrupción de datos se puede considerar como DoS (denegación de servicio) si el atacante los cambia a algo no reconocido por el receptor, perturbando la comunicación desde el emisor. Esta perturbación puede ser temporal si el atacante se ha centrado en el medio de transmisión entre los dispositivos. Si los datos almacenados en las etiquetas o en el almacenamiento de los dispositivos móviles se dañan, esa etiqueta en particular no será válida y se requerirá que el dispositivo móvil obtenga los datos otra vez.

Otro modo de corrupción de datos puede ser mediante la transmisión de frecuencias iguales o válidas en el momento en que los dispositivos legítimos intentan comunicarse entre sí. Este ataque puede ser realizado por software malicioso que se ejecuta en el mismo teléfono inteligente en segundo plano. Este tipo de ataque no corrompe los datos originales, pero los datos recibidos en el extremo del receptor sí se corrompen, siendo un ataque DoS.

Los dispositivos NFC están diseñados para poder detectar los campos de RF en los que se comunican. Si estos dispositivos pueden detectar la fuerza de un campo de RF y la diferencia cuando hay algún RF adicional en el mismo campo, se puede contrarrestar a este tipo de amenaza de forma efectiva. Se requiere una cantidad de potencia superior a la potencia del campo de RF para corromper los datos que se transmiten. Los dispositivos NFC deberían poder detectar fácilmente el aumento de potencia. Estos tipos de ataques se pueden detectar con relativa facilidad y, por tanto, pueden contrarrestarse.

b) Modificación de datos:

En este caso el atacante también cambia los datos reales, pero no con datos desconocidos como en el primer caso de corrupción de datos, sino con datos válidos pero incorrectos. El receptor en este caso recibe datos manipulados por el atacante durante su transmisión. El ataque requiere que el atacante tenga experiencia en el campo de la comunicación inalámbrica y de radio donde pueda controlar y manejar de algún modo la transmisión.

La posibilidad de transferir ondas de radio sobre la parte superior de la forma de onda "legítima" y sincronizar la transferencia de estas es la vulnerabilidad a explotar.

Las modificaciones de datos se pueden proteger de varias maneras. Una de las formas es cambiar la tasa de baudios. Ello puede detener las modificaciones en el modo activo y hacer imposible que un atacante modifique los datos. Sin embargo, esta implementación requeriría el uso del modo activo en ambos extremos. Esto es práctico, pero aumenta las posibilidades de *eavesdropping*.

Los dispositivos NFC son capaces de verificar el campo de RF antes de transmitir los datos. El dispositivo de envío necesita monitorearlo continuamente para detectar la posibilidad de tal ataque y contrarrestar sus efectos. La mejor solución para defenderse de los ataques de modificación de datos es utilizar un canal seguro para la transmisión y recepción de los datos.

c) Inserción de datos:

Un atacante puede insertar datos falsos no deseados en forma de mensajes en los datos legítimos mientras se produce la comunicación entre dos dispositivos. El éxito del atacante en esta manipulación depende de la duración de la comunicación y el tiempo de respuesta del receptor (el atacante necesita responder a los dispositivos antes de que el dispositivo legítimo quiera establecer su comunicación), dado que si ambos dispositivos, el legítimo y el falsificado, transmitieran a la vez, los datos recibidos en el extremo del receptor se corromperían.

Al igual que en la modificación de datos, la posibilidad de transferir ondas de radio sobre la parte superior de la forma de onda "legítima" y sincronizar la transferencia de estas es la vulnerabilidad a explotar.

Una posible contramedida es posible si el dispositivo que responde contesta al primer dispositivo sin ninguna demora. El atacante no tiene ninguna ventana temporal para insertar datos maliciosos o manipulados.

Se puede lograr otra contramedida a la inserción de datos por parte del atacante si el segundo dispositivo, que está en el extremo de escucha, escucha y monitorea continuamente el canal. Los intentos de inserción de datos por parte del atacante pueden ser detectados por el dispositivo que responde.

Pero, sin embargo, la mejor manera de contrarrestar el ataque de inserción de datos es también el uso de un canal seguro para la comunicación mediante la aplicación de algoritmos como RSA, SHA, o un canal inseguro 3DES.

d) Ataque *Man-in-the-middle*:

En el ataque *Man-in-the-Middle* (MITM), un tercero engaña a las dos partes legítimas de la comunicación para hacerles creer que él es la otra parte legítima respectivamente de las dos partes legítimas y, por lo tanto, enruta la comunicación entre las dos partes para que pase por ese tercero.

La vulnerabilidad que se puede explotar en este caso es que la transacción se produzca sin ningún tipo de encriptación.

Las dos partes legítimas no saben que están hablando entre ellas a través del tercero, quien escucha su conversación completa sin que nadie se dé cuenta. Si reemplazamos el enlace entre los dos comunicantes legítimos por NFC, este puede interceptar fácilmente la comunicación entre las dos partes legítimas. La recepción de datos por parte de las dos partes legítimas de la comunicación queda a discreción del dispositivo NFC, quien si lo desea puede bloquear la comunicación entre ellas y, alternativamente, puede enviar mensajes de su elección a cualquier lado, sumando además que puede almacenar, siempre de forma silenciosa, los datos que se transmiten entre las dos partes.

Como se vio anteriormente, la distancia a la que operan los dispositivos NFC es muy corta es decir, 10 cm. Por ello, un ataque MITM es prácticamente imposible de llevarse a cabo a una distancia tan corta. Se recomienda entonces que el modo de comunicación para la NFC sea activo-pasivo, estando evidentemente un dispositivo en cada estado. El dispositivo activo debe monitorear el campo de RF en busca de cualquier posible perturbación o escenario de ataque.

Igualmente, una posible solución es la encriptación de los datos mediante una clave conocida por ambos lados de la comunicación.

3. Ataques que afectan a la disponibilidad:

a) Denegación de servicio:

La denegación de servicio es un ataque cuyos objetivos son los recursos

del servidor de red o la memoria [21]. En este caso se impide el acceso a información o servicios del usuario autorizado [22]. Los patrones más reconocibles de este ataque son irrumpir en el sistema y hacer que no esté disponible y luego intentar robar información valiosa, como la información de la tarjeta de crédito.

Para protegerse de este ataque deberían controlarse varios tipos de técnicas para encender la función de lectura/escritura del dispositivo NFC.

b) Ataque de destrucción:

Es el ataque más simple que podría ocurrirle a la etiqueta NFC que es su inutilización. Después de este ataque, la etiqueta ya no puede comunicarse con un dispositivo NFC. Se puede destruir la tarjeta tanto cortando la conexión a su antena o destruyendo los circuitos eléctricos de la etiqueta.

Este tipo de ataque también afecta a la disponibilidad del sistema, interrumpiendo o corrompiendo los datos para así bloquear el canal de comunicación.

Para protegerse de estos ataques debe incorporarse un cifrado o una forma de controles de validación de datos.

c) Ataque de eliminación:

Se elimina la etiqueta NFC del objeto portador de la misma.

Afecta, efectivamente, a la disponibilidad del sistema. También interrumpe o corrompe los datos para así bloquear el canal de comunicación.

Para protegerse de estos ataques debe incorporarse un cifrado o una forma de controles de validación de datos.

d) Ataque de interferencia:

Interferencia del sistema NFC mediante el envío de una señal que se sitúa cerca del sistema o usando antenas. Este ataque ocurre en el medio inalámbrico y hace que el sistema no esté disponible, modificando o eliminando la información que se envía. No deja de ser un modo de corrupción de datos que ataca a la integridad, además de un ataque más propiamente a la disponibilidad.

La solución más asumible es el incremento de la potencia de la señal del dispositivo para estar por encima de la potencia del atacante y así poder reducir la influencia de la interferencia.

Capítulo 3

Estaciones de recarga del coche eléctrico (EVSE)

En la próxima década se espera un gran crecimiento de los vehículos eléctricos enchufables (EV) en el mundo. El calcula que en la próxima década habrá en circulación unos 120 millones de coches eléctricos. En lo que corresponde a España, actualmente se calcula que, en el mejor de los casos, no disponemos de más de 674 mil automóviles tanto eléctricos como híbridos. El equipo de carga, también conocido como EVSE o estación de carga, proporciona carga segura a los vehículos eléctricos, de manera similar a las estaciones de servicio.

Actualmente, una de las limitaciones más graves para la difusión del EV es la falta de una infraestructura de carga de EV generalizada, a pesar de la gran difusión de la infraestructura eléctrica. Aunque se espera que el problema del coste de los EV disminuya con su creciente difusión (lo que va produciendo una mayor investigación y avance en este tipo de tecnologías), la todavía limitada autonomía del automóvil y el aún largo tiempo de carga de la batería, mucho más prolongado en comparación con el que se tarda en llenar el depósito de combustible de los vehículos de combustión interna [25], son percibidos actualmente por los compradores como serias barreras a la compra [26] [27].

Por ahora, el tiempo de recarga de la batería está limitado principalmente por la capacidad de la conexión a la red. Si bien la recarga mediante enchufes puede realizarse durante la noche en el hogar, es posible realizar una solución de recarga más rápida que requiere una alta potencia para la red eléctrica en estaciones de recarga, en estacionamientos públicos o comerciales, en centros comerciales y en la calle o los lugares de trabajo.

Con una difusión masiva del EV, las cargas de las baterías tendrán un gran impacto en el funcionamiento de las redes inteligentes, por lo que se debería tener en cuenta la alta potencia necesaria para una carga rápida (por ejemplo, se requieren 150 kW para cargar un Tesla modelo S del 20 % al 80 % en 30 minutos). Los problemas de sobrecarga de la red eléctrica pueden surgir cuando varios vehículos en el mismo vecindario se recargan al mismo tiempo, o durante los picos de carga normales.

Los sistemas de carga de coche eléctrico no dejan de ser un tipo de CPS. Estos CPS son sistemas construidos mediante una integración segura y sin inconvenientes físicos y de computación (es decir, detección, computación y redes). Las llamadas tecnologías de sistemas inteligentes, como el transporte inteligente, la red inteligente, los vehículos inteligentes... se basan en los fundamentos de esta integración de CPS. La carga inteligente proporciona un mecanismo de comunicación entre el EVSE y la red que admite el monitoreo y la gestión de energía para mejorar la eficiencia y la personalización de los horarios de carga. A través de una mejor conectividad y control estos protocolos de carga inteligente han sido diseñados para reducir costes, equilibrar las cargas máximas y facilitar una mejor integración con diferentes niveles de operadores de red y fuentes de energía renovable. Los EVSE existentes tienen varios componentes tanto de comunicación como informáticos los cuales se utilizan para gestionar y controlar su funcionamiento. Por otro lado, las tecnologías emergentes de redes inteligentes también tienen como objetivo el facilitar un intercambio de energía bidireccional entre los vehículos eléctricos enchufables y la red a través de EVSE, en particular los cargadores rápidos. Además durante el proceso de autenticación para el inicio de la recarga inteligente se envían tanto la información personal como la financiera. Por todo ello, que la operación de EVSE sea segura es muy importante tanto para los vehículos como para las personas y la infraestructura de la red eléctrica.

Hay varias posibles motivaciones para lanzar un ataque a una estación de carga que van desde el robo de electricidad hasta algunos ataques más sofisticados buscan producir la interrupción de una red de estaciones de carga mediante el uso de un EVSE como punto de entrada a la misma. Los ataques podrían ser aún más graves si el malware consigue propagarse potencialmente a través de una red de estaciones de carga que pudieran afectar la red eléctrica.

La Sociedad de Ingenieros Automotrices (SAE) ha desarrollado un conjunto de estándares y protocolos para ser implementados por los fabricantes de estaciones de carga. La cantidad de componentes interconectados en EVSE y la conectividad

de este con otros subsistemas (vehículos, smartphones, la red eléctrica...), y los mecanismos de seguridad mal implementados hacen que EVSE sea muy vulnerable a los ataques cibernéticos. El Departamento de Energía/Departamento de Transporte de los Estados Unidos (DOE/DOT) realizó un informe el cual destaca brechas de seguridad cibernética en la infraestructura EVSE actual que incluye ataques de intermediarios o terceras personas, fraude de pagos, privacidad, daños a la batería del vehículo, degradación de servicio (DoS) y el malware se propaga del vehículo eléctrico o EV al EVSE. El informe antes mencionado y algunos otros estudios [28] [29] [30] demostraron algunas brechas y deficiencias en la infraestructura de carga existente por la falta de guías a seguir y pruebas de seguridad cibernética realizadas antes de su implementación. Además también indican algunos estudios cómo la carga descontrolada de EVSE puede crear un desequilibrio o un efecto negativo en la red eléctrica.

3.1. Seguridad de los dispositivos EVSE desde un punto de vista ciberfísico

Actualmente, la mayoría de las estaciones de carga ya implementan algún tipo de seguridad de la información. Pero, en cualquier caso, estos métodos basados en tecnología de la información están limitados con respecto a la comprensión de cómo puede verse afectada la seguridad general de CPS. Relacionando los objetivos de ciberseguridad generales con los de este sistema encontramos lo siguiente:

1. *Disponibilidad*: Está determinada por el tiempo activo frente al tiempo de inactividad de los servicios de carga. Es importante que se proporcione un sistema defensivo para monitorizar, detectar y prevenir ataques DoS, entre otros tipos de ataques a las estaciones de carga, para mantener una alta disponibilidad.
2. *Integridad*: Es la protección contra cambios no autorizados, ya sea en los datos como en la información de control. La protección debe proporcionarse contra la manipulación de la información almacenada o intercambiada entre varias entidades, ya sea la estación de carga, el servidor centralizado o el dispositivo del cliente.
3. *Confidencialidad*: Garantiza el mantenimiento del secreto en la transmisión de datos entre las partes, ya sean datos del usuario o información bancaria.

Los principales tipos de EVSE son el Nivel 1 (120V de corriente alterna, en adelante CA, monofásico de “carga lenta”), el Nivel 2 (240V de CA de fase dividida) y el Nivel 3 (hasta 500V de corriente continua, en adelante CC). El hardware de los EVSE de nivel 2 diseñados para su uso en estaciones de carga disponibles públicamente es bastante más complejo que los cargadores de nivel 1 y los EVSE de nivel 2 diseñados para uso doméstico privado. La disponibilidad de un hardware informático más sofisticado también permite que el EVSE de nivel 2 tenga un mayor número de protecciones de seguridad para la carga que la mayoría de los EVSE de nivel 1. Más allá del equipo necesario para iniciar la recarga de CA, el EVSE de nivel 2 en las estaciones de carga requiere placas de circuito impreso patentadas para controlar una variedad de componentes y subsistemas. Muchos EVSE de nivel 2 tienen módulos de comunicación que se utilizan para conectarse con una red de comunicaciones de forma inalámbrica, lo que permite a los fabricantes implementar una serie de funciones, como validación y verificación de usuarios, establecimiento de tarifas por parte del administrador de la estación de recarga y el reporte de eventos tales como información de diagnóstico, inicialización y finalización de recargas...

Los EVSE en las estaciones de carga de nivel 2 suelen disponer de indicadores LED y LCD que se utilizan para proporcionar a los usuarios información sobre el estado de la estación y/o la en qué estado se encuentra su proceso de carga, algo similar a las bombas de gasolina modernas. También es común que EVSE venga equipado con escáneres de identificación por radiofrecuencia (RFID) que pueden leer tarjetas de crédito o tarjetas de miembros de la red EVSE para poder procesar pagos. EVSE puede implementar varias placas con algunos propósitos especiales, ya sea una placa de comunicación, una placa de LED o una placa de E/S de usuario.

El tener un hardware más sofisticado permite que el EVSE de nivel 2 pueda incluir más protecciones de seguridad para el proceso de recarga que la mayoría de los EVSE de nivel 1. Al igual que el EVSE de nivel 1, el EVSE de nivel 2 interactúa con los EV a través de un conector de cinco conductores. Tres de los cables están conectados para suministrar energía desde la red eléctrica y solo están separados de una conexión directa de red al EV a través de relés internos del EVSE. Se utiliza una combinación de tres tomas de voltaje conectadas directamente además de tres sensores de transformadores de corriente no invasivos que proporcionan al hardware de la computadora principal del EVSE información sobre la energía entregada a un vehículo conectado al punto de recarga, lo que permite las mediciones necesarias utilizadas para calcular el coste de la sesión de recarga. Los otros dos cables son la línea piloto y la línea de proximidad. La línea de proximidad se conecta solo a una

red de resistencia simple dentro del enchufe EVSE que es la que el EV utiliza para determinar si la conexión está bien realizada. Normalmente no se comunica con el hardware de la computadora EVSE de ninguna manera, aunque algunos modelos incluyen componentes electrónicos en el circuito que evitan que se notifique en el extremo EV que la conexión se ha realizado correctamente cuando el EVSE no está listo para recargar. El cable más importante es la línea piloto, que es el que utilizan el EVSE y el EV para comunicarse entre sí. Cuando una estación está inactiva, se aplica una señal de voltaje de 12V CC a la línea piloto, pero cuando un EV consigue conectarse mediante una conexión física, el EVSE detecta esta acción a través de un detector de voltaje y cambia a una fuente que genera una onda cuadrada de 1kHz de amplitud de 12V en la línea piloto. Después, un circuito eléctrico en el EV que consta de interruptores y resistencias responde a EVSE cuando se detecta esta onda cuadrada y el EVSE puede comenzar un proceso de recarga. Si se produce un problema eléctrico en el lado de la red del EVSE o si es el propio usuario el que desconecta repentinamente su vehículo del EVSE en medio de una sesión de recarga, el hardware de la computadora EVSE abrirá los relés en una fracción de segundo, eliminando la energía del adaptador para evitar cualquier tipo de daño al usuario.

El hardware de la computadora y el sensor de Level 3 EVSE es como el de Level 2 EVSE. Dos de los tipos principales de estaciones de carga rápida de CC son las que utilizan la expansión del estándar de carga combinada (CCS) y las que siguen el protocolo japonés CHAdeMO, junto con los supercargadores patentados de Tesla Motor, que solo funcionan con sus propios vehículos, siendo el tercero más influyente. Las principales diferencias entre los EVSE de nivel 2 y 3 se reducen a la ubicación del circuito del cargador, el método de comunicación por cable entre el EV y el EVSE, y el diseño del adaptador físico. Aunque se utiliza habitualmente de forma errónea el término "cargador" para referirse a EVSE en publicaciones, todos los EVSE de nivel 3 que están en el mercado ya contienen rectificadores de CA-CC y otros circuitos de carga dentro del propio EVSE, mientras que la recarga de nivel 2 requiere dichos circuitos dentro del EV. Los conectores físicos para CCS EVSE son esencialmente conectores modificados que incluyen dos pines grandes que se usan para la entrega de energía de CC. CCS EVSE puede utilizar la línea piloto igual que el EVSE de nivel 2, aunque este conductor se puede utilizar también para la comunicación por línea eléctrica (PLC) con la red inteligente. Los conectores CHAdeMO EVSE cuentan con un conjunto similar de dos pines grandes al adaptador CCS, pero también tienen una mayor cantidad de pines en total. Tres de estos son pines de control de sesión de carga que funcionan de igual forma que la línea piloto, pero dos de los pines se usan

para facilitar la comunicación de la red de área del controlador con los vehículos, lo que habilita una comunicación por cable más compleja.

3.2. Tipos de ataques centrados en dispositivos EV-SE

Una superficie de ataque es un punto de entrada a través del cual se pueden lanzar multitud de ataques. Hay dos categorías diferentes de puntos de entrada que podrían usarse para comprometer la seguridad de un EVSE: los físicos (utilizando el puerto de carga, manipulando el hardware de los dispositivos...) y los basados en la red.

3.2.1. Ataques basados en la red

Habitualmente los cargadores de nivel 2 y nivel 3 son equipados con algún módulo de comunicación con una interfaz inalámbrica (Bluetooth, Wi-Fi...) o por cable. Este módulo de comunicación permite a los usuarios autorizados iniciar una sesión de recarga y a la propia estación de recarga comunicar su estado propio o el estado de la sesión de recarga al operador de la misma estación. Esta comunicación se produce a través de módulos en el vehículo, un teléfono inteligente o una tarjeta RFID. Las vulnerabilidades de las comunicaciones de corto y largo alcance están bien documentadas en la literatura [11-14]. Poner en peligro la seguridad de cualquiera de estos puntos finales de la red (es decir, BEMS, el servidor del controlador y la interfaz de operación de la estación) debido a una mala autenticación o falta de cifrado tiene el potencial de afectar a todas las estaciones de carga conectadas al nodo final. Esto tiene el potencial de comprometer la confidencialidad e integridad tanto de los datos como de los comandos de control, lo que afecta la disponibilidad de la estación de carga, el controlador de la estación de carga (o interfaz de gestión), el servidor BEMS y/o la red eléctrica. Una lista de posibles ataques basados en la red es la siguiente:

1. *Suplantación de identidad*: La mayoría de las comunicaciones basadas en protocolos de comunicación inalámbrica (RFID, Bluetooth, Wi-Fi...) pueden sufrir este tipo de ataques. Una forma común de este ataque es comprometer el identificador único del dispositivo (por ejemplo, la etiqueta RFID) y hacerse pasar por ese usuario (por tanto, un usuario legítimo). Esto suele ocurrir antes de

que se establezca el cifrado y se generen las claves. Este tipo de ataques tienen la capacidad de comprometer la identidad del usuario (por tanto, atacar a su privacidad) y de modificar los datos transmitidos (atacar a la integridad de ellos). Para realizar un ataque por ejemplo se utilizaría la identidad del usuario para, por ejemplo, realizar la recarga en el nombre de otra persona o incluso para poder lanzar ataques DoS, los cuales se verán más adelante.

2. *Man-in-the-Middle (Hombre en el medio, MITM)*: El atacante trata de bloquear el receptor mientras puede acceder al tráfico transmitido, lo que permite que el atacante actúe como un punto intermedio entre el emisor y el receptor sin que ninguna de las partes lo sepa. La mayoría de las comunicaciones basadas en radio son propensas a estos ataques MITM. Estos pueden ocurrir entre los nodos (por ejemplo EVSE y EV). El atacante podría corromper los datos o tomar el control completo del nodo y alterar el estado de uno de ellos para por ejemplo transmitir información incorrecta (por ejemplo notificar en la estación de recarga un error que no existe). Si las comunicaciones o el código fuente no se ofuscan o encriptan los ataques MITM son más fáciles de ejecutar.
3. *Denegation of Service (Negación de Servicio, DoS)*: Si se comprometen las credenciales del usuario, el propio usuario y la estación se podrían utilizar para lanzar ataques DOS muy sofisticados. Por ejemplo, las credenciales de usuario se pueden usar para lanzar este tipo de ataques contra nodos. Los posibles ataques a considerar son la inundación UDP o TCP/IP, DoS de baja velocidad, inundación de ping o inundación ICMP. Estos ataques son capaces pueden deshabilitar una estación de carga u otros nodos situados en la misma red de la estación de carga.
4. *Ataque de inyección SQL*: Explota una base de datos con una implementación no del todo correcta para insertar, actualizar o eliminar datos de la propia base de datos. Esto haría que un atacante pueda ejecutar comandos que afecten a, entre otras cosas, la capacidad de recarga de los usuarios, imposibilitar el acceso a algún usuario, cambiar la disponibilidad de una estación, robar datos económicos... lo que puede causar problemas de seguridad o económicos.
5. *Ataque de malware*: Explota una mala implementación de seguridad de varios de los módulos de software en la estación de carga y/o en la nube para lanzar ataques más sofisticados que instalen algún tipo de malware. Por ejemplo, un malware con potencial de lanzar un ataque más coordinado podría provocar el

cierre de una red de estaciones de carga o hasta afectar a toda la red eléctrica porque se podrían activar varias estaciones de carga simultáneamente.

3.2.2. Ataques físicos

En teoría, un atacante que disponga de acceso físico a un EVSE podría recoger información de la placa de la estación de carga para espiar las comunicaciones entre componentes. Esto se podría hacer manipulando físicamente la estación de carga si la resistencia a ella es débil. Dado que cada tipo de EVSE tiene una arquitectura diferente, el atacante debe estudiar diferentes componentes, comprender varios módulos de comunicación de la estación de carga y tener algún tipo de microcontrolador y varias herramientas de rastreo o sondeo para obtener información valiosa de su acceso físico a la estación de carga. La complejidad de la arquitectura varía mucho entre cada tipo de EVSE. Todas las estaciones de carga de nivel 2 y nivel 3 tienen un microcontrolador para controlar las funciones requeridas por un EVSE, y muchas están equipadas con un sistema operativo en tiempo real que habitualmente ejecuta un núcleo Linux. Existen varias herramientas de hardware para extraer firmware a través de las interfaces *Universal Asynchronous Receiver- Transmitter* (UART) o *Joint Test Action Group* (JTAG). Los tipos específicos de ataques incluyen los siguientes:

1. *Físicos y de canal lateral*: Implican obtener acceso a los componentes de nivel de chip para manipular e interferir con las partes internas del sistema. Junto con este tipo de ataque, los hay de canal lateral que implican la ingeniería inversa de un chip al observar información de tiempo, consumo de energía y fugas electromagnéticas. Con esta información, es posible recuperar datos confidenciales, como por ejemplo claves de cifrado utilizadas en las comunicaciones o datos que se transmiten a través de la electrónica de la estación de recarga. Estos ataques son muy difíciles de implementar y requieren equipos con un coste elevado.
2. *Basados en interceptación*: Implica el espionaje de datos confidenciales, lo que compromete la privacidad y confidencialidad del usuario. Esto se logra mediante el uso de técnicas de sondeo para acceder y monitorear los datos en los puertos del hardware físico. Además se puede usar también para interceptar algún tipo de información enviada al EVSE, lo que podría alterarla antes de que se envíe al sistema.

3. *Basados en modificación:* Compromete integridad del software mediante la explotación de las vulnerabilidades detectadas. Por ejemplo, el acto de usar un desbordamiento de búfer para sobrescribir la memoria de la pila, dirigiendo el control hacia algún programa de tipo malware, constituiría un ataque de modificación.

3.2.3. Ataques híbridos

Mediante el uso de varias combinaciones de ataques basados en la red y ataques físicos, es posible lanzar ataques aún más sofisticados. Por ejemplo, si un atacante tuviera acceso al servicio en la nube, se podría autorizar un EVSE para iniciar una sesión de recarga con un vehículo manejado por un usuario no autorizado. Para los EVSE que carecen de un protocolo de enlace EV-EVSE correctamente implementado al contacto, la modificación física del enchufe del adaptador del EVSE permite activar una sesión de carga de Nivel 2 sin la presencia de 1 vehículo. La combinación de ambos ataques permite que el enchufe del adaptador de la estación de carga se active remotamente, lo que podría permitir que algunos dispositivos distintos a los EV reciban energía a través del EVSE, pudiendo utilizarse esto para cualquier fin.

Los diferentes ataques que pueden realizarse a partir de la combinación de ataques físicos y cibernéticos a la red pueden ser increíblemente perjudiciales para el funcionamiento normal de un EVSE y la seguridad de los usuarios.

3.3. Enfoques para mejorar la seguridad CPS

Se están implementando e instalando una gran cantidad de puntos de recarga, de momento con estándares limitados para aportar seguridad a este tipo de infraestructuras. Dado que la seguridad y la disponibilidad de las estaciones de carga afectan indirectamente tanto a la red eléctrica como al sector del transporte, es importante disponer de unas bases sólidas de ciberseguridad para poder implementarlas. Algunas de ellas se adoptaron de las mejores prácticas de seguridad del sistema integrado, pero la mayoría de ellas son exclusivas de las propias estaciones de carga.

3.3.1. Seguro por diseño

El diseño de una estación de carga segura va mucho más allá de asegurar los componentes individuales del sistema. Esto se debe a que las estaciones de carga interactúan con múltiples sistemas, entre ellos vehículos, smartphones, la infraestructura energética y la nube. Esto lo que hace es aumentar los vectores de amenazas, los cuales los atacantes pueden explotar. El diseño de seguridad de la estación de carga debe identificar todos los posibles vectores de amenazas (tanto cibernéticos como físicos), así como las vulnerabilidades y el riesgo que las amenazas supondrían para las personas, los vehículos y la infraestructura. Este diseño debe incluir componentes tanto de hardware como de software. Los diseñadores de EVSE deben tener en cuenta la variedad de posibles amenazas y considerar las estrategias necesarias para limitarlas. Varios modelos gráficos y formales como Petrinets, diagramas de flujo de datos, simulaciones de eventos discretos o los modelos CPS [31] [32] [36] [37] se pueden utilizar para verificar y evaluar las propiedades de seguridad y protección del diseño. Es necesaria además la existencia de un aislamiento limpio en el hardware y el software para evitar el acceso no autorizado o el espionaje de la información protegida y las señales de control.

3.3.2. Seguridad del software

La estación de carga incluye software que se ejecuta en la placa que envía las señales de control a la propia estación de carga, la interfaz de administración de la propia estación de carga, las aplicaciones móviles y la interfaz de programación de aplicaciones proporcionada por las estaciones de carga. La mayoría de estas estaciones también ofrecen un servidor que se comunica con la estación a través de Internet. Los principios de seguridad por diseño se aplican a la arquitectura de software para la estación de carga para identificar las lagunas de seguridad que hacen que estos sistemas sean vulnerables [31]. Dada la integración compleja y estrecha de hardware y software, algunos de los ataques de software también se pueden realizar a través del hardware. Hay muchas contramedidas disponibles para autenticar y validar el software en diferentes pasos, como por ejemplo evitar la manipulación del software y asegurar el arranque.

3.3.3. Seguridad del hardware

Los microprocesadores que se utilizan en las estaciones de carga suelen tener una potencia computacional baja la cual es incompatible con implementar un cifrado fuerte. El agregar coprocesadores seguros como aceleradores de hardware criptográfico [32] reducirá las opciones de manipulación del hardware. Los coprocesadores seguros brindan soporte criptográfico de alto rendimiento que almacena claves de manera mucho más segura a pesar de los posibles ataques físicos o lógicos.

3.3.4. Supervisión y resistencia a la manipulación

El software malicioso también puede aprovechar las lagunas del software y del sistema operativo para instalar malware que afecte al funcionamiento normal del sistema. Las medidas de resistencia a la manipulación para proteger contra ataques físicos y de canal lateral incluyen protección física para evitar la manipulación, encriptación de BUS, implementación de circuitos donde las características de potencia son independientes de los datos y blindaje de los chips en la placa. Además de la protección contra manipulaciones, también es importante monitorizar y registrar las actividades críticas para prevenir e investigar algunas vulnerabilidades relacionadas con la seguridad cibernética.

3.4. OCPP

La estandarización de los protocolos de comunicación para la movilidad eléctrica es necesaria para garantizar que el rendimiento, la seguridad y la protección sean los mismos que los del vehículo convencional real. Las principales organizaciones que desarrollaron estándares para los EV son la Comisión Electrotécnica Internacional (IEC), la Sociedad de Ingeniería Automotriz (SAE), y otros consorcios públicos y empresas privadas de vehículos eléctricos que desarrollan estándares abiertos.

Existen diferentes estándares en continuo desarrollo en lo que respecta a la comunicación entre los EV y los EVSE. Los principales estándares son [33] [34]:

1. *SAE J2931, SAE J2836, SAE J2847, SAE J1772*
2. *CEI 61850-7-420, CEI 62196, CEI 61851, CEI 15118*
3. *OCPP, OICP, OCHP*

Para la realización del trabajo se utilizará el protocolo OCPP. OCPP [34] [35] es un estándar abierto creado por Open Charge Alliance (OCA), que consiste en un consorcio de varias organizaciones públicas y privadas.

OCPP es el estándar respaldado de facto por la industria para la comunicación entre una estación de carga y un CSMS y está diseñado para adaptarse a cualquier tipo de técnica de carga [35].

El objetivo de OCA es favorecer el desarrollo de una infraestructura de red con la creación de un protocolo abierto, libre e independiente de las características de cada fabricante individual, y que permita la gestión de todas las situaciones de una operación de recarga. El OCPP tiene como objetivo realizar una serie de operaciones entre componentes que representan dispositivos físicos involucrados en la operación de recarga. Estas operaciones se realizan mediante el intercambio de uno o más mensajes denominados Protocol Data Unity (Unidad de Datos de Protocolo, PDU).

La versión 1.5 de OCPP, de junio de 2012, es capaz de:

1. Monitorizar y controlar el acceso a las estaciones de carga individuales.
2. Consultar y gestionar el estado de la recarga.
3. Enviar datos a usuarios y administradores.
4. Permitir el procedimiento de pago.
5. Permitir mecanismos de reserva y gestión eléctrica.

En estos últimos años, el protocolo OCPP se ha ido modificando para tener en cuenta los requisitos emergentes de las redes inteligentes, además de para aumentar la participación del usuario en el proceso de carga.

Una característica fundamental añadida en la versión 1.6, la cual fue lanzada en octubre de 2015, es “Smart Charging” (carga inteligente”). Con “Smart Charging”, el Sistema Central es capaz de modificar la potencia de carga de un EV específico o el consumo total de energía permitido en todo un punto de recarga siempre en base a la disponibilidad de energía en la red. El Sistema Central recibe el pronóstico de demanda/solicitud de energía del operador de la red y, tras ello, modifica los tiempos de carga para algunas o todas las transacciones de carga. Las características de carga y los tiempos se definen en el tipo de “ChargingProfile” (perfil de carga), el cuál describe la cantidad de corriente o potencia que se puede entregar en un intervalo de tiempo. Aunque el “ChargingProfile” puede estar relacionado con una sola transacción de carga, el usuario no tiene un rol activo en su definición.

Algunas de las mejoras más relevantes de OCPP 2.0, lanzado en marzo de 2018, son las siguientes:

1. Ciberseguridad.
2. Soporte de la norma ISO 15118.
3. Se obligó a la existencia de diferentes opciones de autorización del cliente (tarjeta/token RFID, ISO 15118-1 Plug and Charge, terminales de pago, llave mecánica local, teléfonos inteligentes, etc.).
4. Se obliga a mostrar mensajes en la estación de carga para que los vean a los conductores de EV (relacionados con la transacción, el idioma que se utilizará, sobre la tarifa aplicable antes de que el conductor de EV comience a cargar, para mostrar el coste de funcionamiento durante y al final de una transacción de carga...).
5. “Smart Charging” extendida.

El Extended Smart Charging intenta optimizar la gestión de la energía teniendo en cuenta los límites del proveedor de energía, o las limitaciones de una energía sostenible a partir de paneles solares en el caso de que hablamos de un suministro local. Esta gestión inteligente se obtiene gracias a la flexibilidad del “ChargingProfile”. La versión 2.0 del protocolo OCPP amplía las características del “ChargingProfile”. Un CSMS puede enviar un “ChargingProfile” a una estación de carga, usando el mensaje “SetChargingProfileRequest” (establecimiento de solicitud de perfil de carga) en estas situaciones:

1. Al comienzo de una transacción para establecer el perfil de cobro para la misma.
2. En una solicitud RequestStartTransaction (solicitud de inicio de transacción) enviada a una estación de carga.
3. Durante una transacción para cambiar el perfil activo para la misma
4. Fuera de un proceso de transacción como un mensaje separado.

Sin embargo, el protocolo OCPP 2.0 todavía no considera las solicitudes del conductor en el “ChargingProfile”. OCPP 2.0.1, publicado el 8 de abril de 2020, reemplaza a OCPP 2.0 y presenta varias correcciones de errores y mejoras basadas en las experiencias adquiridas en el funcionamiento de OCPP 2.0. Algunas de estas mejoras están a nivel de mensaje. Se han realizado mejoras en el área de seguridad,

en el cumplimiento de ISO 15118, en Smart Charging y en la extensibilidad de OCPP.

1. Smart charging: siguiendo las funciones de carga inteligente, el EV proporcionará las necesidades de carga (hora de finalización de la recarga y energía solicitada). El CSMS puede proporcionar hasta tres horarios con diferentes tarifas y el EV elige un horario. El perfil de carga se puede cambiar durante la transacción (esto recibe el nombre de “renegociación”).
2. Reserva: el protocolo OCPP le permite hacer una reserva de un EVSE o un tipo de conector de un EVSE específico. La reserva se realiza hasta una hora determinada. El usuario puede realizar una reserva sobre los recursos del EVSE que estén disponibles en el momento de la reserva. El usuario no puede realizar una reserva anticipada, es decir, reservar por ejemplo para dentro de una hora durante las tres horas siguientes.
3. Tarifa y coste: el protocolo OCPP permite mostrar la tarifa al usuario antes de iniciar la transacción, durante y al final de la misma.

En esta última versión de OCPP (2.0.1), el CSMS es capaz de proporcionar hasta tres horarios con tarifas diferentes, puede mostrar tarifas y puede aceptar también reservas de tiempo reducido. No se permite, como se explicó anteriormente, la reserva anticipada, algo que es probablemente debido a la complejidad de la gestión de la programación de la reserva anticipada y también a la prioridad que se da al usuario que está realmente presente en el punto de recarga respecto de una reserva remota.

Este trabajo utilizará el protocolo OCPP 1.6, ya que es la que dispone de un uso más extendido actualmente en las plataformas de gestión de los EVSE. La mayor parte de los puntos de recarga que se utilizan actualmente en la red disponen de la posibilidad de aplicar este protocolo.

Capítulo 4

Arquitectura de un sistema basado en OCPP

El protocolo OCPP utilizará WebSocket (WS) como protocolo de comunicación entre las estaciones de carga individuales y el sistema central. Los datos que pasan por WebSocket se pueden formatear en diferentes formatos incluyendo SOAP o JSON. Utilizamos la implementación JSON, que es un formato ampliamente utilizado en varios campos, y se presta para interactuar con aplicaciones web escritas en lenguaje Java y aplicaciones en la plataforma Android. Se puede interactuar también con aplicaciones de otro tipo de lenguaje, como el PHP, desarrollado mayoritariamente en este sistema. El sistema desarrollado para la infraestructura de la recarga del coche eléctrico consta de la propia estación de carga, el sistema de gestión de las estaciones de carga, la base de datos que almacena los datos, el EV y el conductor del EV a través de una aplicación o de un entorno web, en un dispositivo como puede ser un smartphone, una tablet o incluso un PC, o a través de una tarjeta que preguntará al servidor si está o no autorizada.

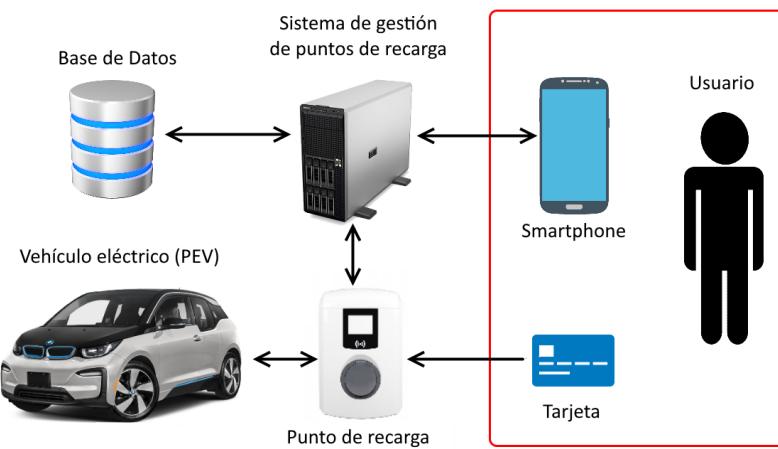


Figura 4.1: Arquitectura del sistema propuesto

1. *Vehículo eléctrico*: El EV crea una comunicación con la estación de carga a través de la línea eléctrica, basándose en el estándar ISO/IEC 15118. En ella, intercambian información sobre la potencia máxima permitida, la capacidad de la batería del vehículo...
2. *Usuario*: El conductor inicia el proceso de recarga a través de una interfaz en el punto de recarga, el uso de algún tipo de tarjeta de fidelización, la utilización de un smartphone o tablet, incluso a distancia desde una interfaz web (también utilizable en un smartphone o tablet) o en algunos casos con un protocolo inalámbrico de amplio rango (por ejemplo, conexión 4G/5G) ya existente en el EV. Además, en algunos casos el conductor puede definir los parámetros de la recarga directamente con el EVSE y monitorear la recarga real. En el caso que se trata, se utilizarán tan solo smartphone (con interfaz web) o con el paso de una tarjeta.
3. *Punto de recarga*: Permite la interoperabilidad con todo tipo de EV, proporciona al usuario distinta información sobre el estado actual del mismo, de la recarga que está realizando o acaba de realizar..., e intercambia información con la base de datos a través del sistema de gestión de puntos de recarga.
4. *Base de datos*: La base de datos almacena datos de los puntos de recargas disponibles en el sistema o en otros sistemas con los que haya algún tipo de acuerdo, de los usuarios autorizados para usar los puntos de recarga, de todas las reservas en estos mismos y la información de facturación... La estructura de la base de datos se tratará más adelante.

5. *CSMS*: Coordina todas las operaciones. Consiste en una aplicación web que maneja las solicitudes tanto del punto de recarga como de la aplicación del usuario del EV e intercambia datos con la base de datos. El servicio de atención al cliente de la estación central es responsable de proporcionar y recibir información de la aplicación del usuario. En particular, la aplicación envía solicitudes HTTP POST al servidor web, que contiene los datos enviados por parte de los puntos de recarga en formato JSON.

4.1. Protocolo OCPP 1.6

En este apartado se definirán en profundidad algunos de los conceptos básicos, en especial en torno a algunas características del funcionamiento, el modelo de intercambio de mensajes, la forma de comunicación... del protocolo OCPP 1.6.

4.1.1. Ejemplos de funcionamiento

Hay dos posibilidades de comunicación entre el punto de recarga y el CSMS en este protocolo. En el primero, es el punto de recarga el que inicia el proceso de comunicación y en la segunda es el CSMS el que lo hace. Dos ejemplos de esto son los siguientes:

1. En el primero, un punto de recarga solicita la autenticación de una tarjeta o de un identificador enviado por el propio CSMS y envía el estado de la transacción de carga.
2. En el segundo caso, es el CSMS inicia la actualización del firmware de un punto de recarga.

El proceso para el inicio y la detención de una recarga se puede ver en el siguiente diagrama:

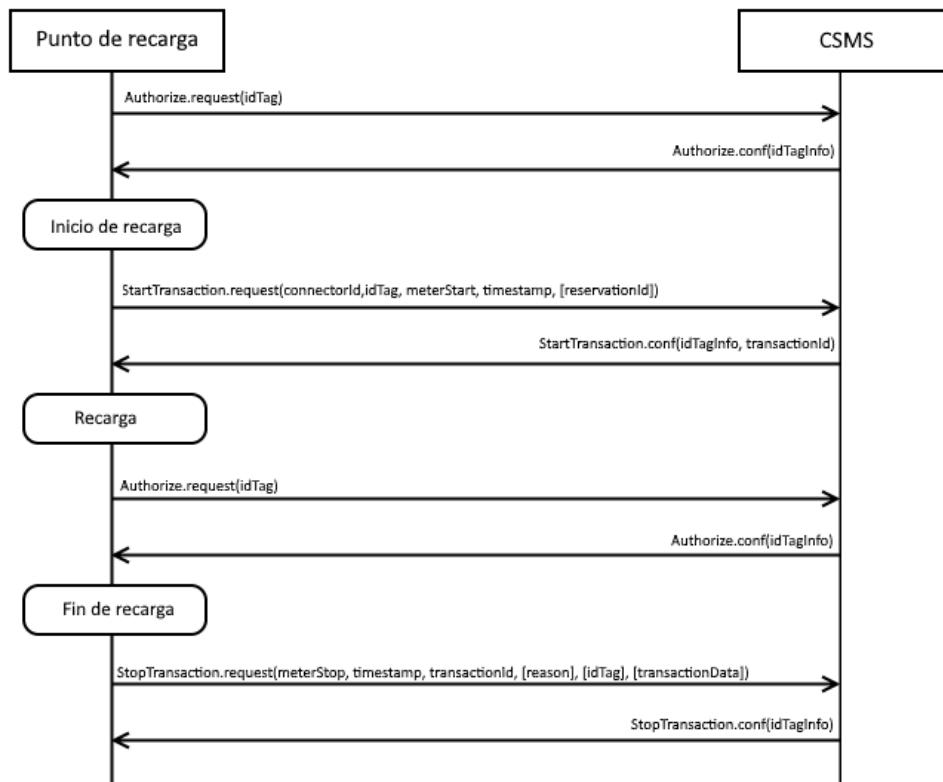


Figura 4.2: Diagrama de secuencia de una recarga

Cuando un punto de recarga va a cargar a un EV, primero debe autenticar al usuario antes de que se pueda iniciar la carga. Si este está autorizado, el punto de recarga inicia la carga e informa al CSMS que ha iniciado la carga.

Cuando un usuario desea finalizar la recarga y desenchufar el EV del punto de recarga, este debe verificar que es el usuario que inició la carga o que es un usuario distinto pero con permiso para finalizar la recarga. Una vez autorizado, el punto de Recarga informa al CSMS de que se ha finalizado la recarga.

El proceso de actualización de firmware es como el visto a continuación:

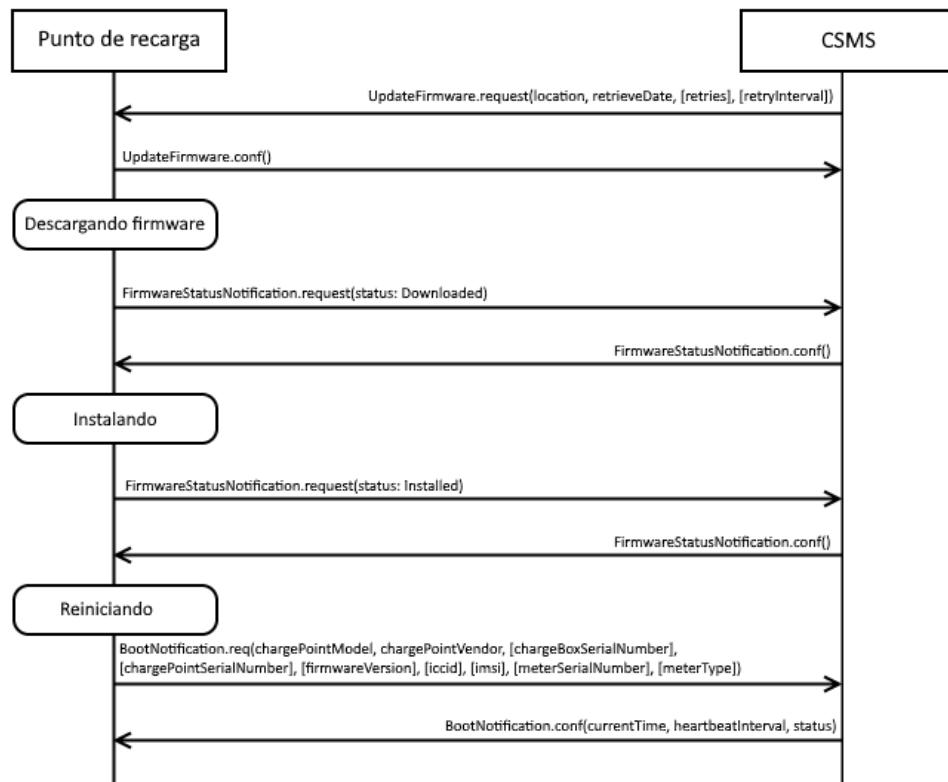


Figura 4.3: Diagrama de actualización de firmware

Cuando un punto de recarga necesita una actualización de firmware, el CSMS informa al punto de recarga de la hora en la que este puede comenzar a descargar el nuevo firmware. El punto de recarga debe notificar al CSMS cada paso realizado a medida que se va descargando e instalando el nuevo firmware.

4.1.2. Modos de autorización local y funcionamiento sin conexión

En caso de no disponibilidad de las comunicaciones a través de internet o una caída del CSMS, el punto de recarga está diseñado para poder funcionar de forma autónoma. En este caso, se considera al punto de recarga *desconectado* y se marca como tal si funciona el CSMS.

Para mejorar la experiencia de los usuarios, se puede configurar un punto de recarga para admitir la autorización local de identificadores a través una caché de autorización y/o una lista de autorizaciones locales (*whitelist*). Otra opción es el

permitir recargar a todo el mundo en caso de que no haya conexión entre punto de recarga y CSMS.

Esto permite la autorización de un usuario cuando el punto de recarga está desconectado y mejora el tiempo de respuesta de autorización cuando la comunicación entre el punto de recarga y el CSMS es lenta.

Por otro lado, un punto de recarga puede configurarse para admitir la autorización (automática) de cualquier identificador cuando el estado del mismo es de desconectado, para evitar la denegación de servicio y posterior cobro a usuarios de buena fe que no pueden ser autorizados explícitamente por las entradas de la lista de autorización local/caché de autorización. En este caso se desactivará esta autorización automática por motivos de seguridad.

4.1.3. Numeración de conectores

Para que el CSMS pueda comunicarse con todos los conectores de un punto de recarga, los ConnectorIds deben estar siempre numerados de la siguiente manera:

1. El identificador (ConnectorId) del primer conector debe ser 1.
2. Los conectores adicionales deben numerarse de forma secuencial, sin omitir números.
3. Los ConnectorIds nunca deben ser superiores al número total de conectores de un punto de recarga. Si hay tres conectores el número máximo es 3. item Para operaciones iniciadas por el CSMS o por el punto, se reserva el número 0 de ConnectorId para enviar información general al punto de recarga.
4. Para las operaciones iniciadas por el punto de recarga (informativas), el número 0 de ConnectorId está reservado para el controlador principal del punto de recarga.

4.1.4. Identificadores

Los datos adquiridos a través del hardware del lector local de tarjetas suelen ser un valor UID (4 o 7 bytes) de una tarjeta RFID física, representado como 8 o 14 caracteres de dígitos hexadecimales.

Sin embargo, estos identificadores cuando son enviados a los puntos de recarga por los CSMS para las sesiones de carga iniciadas de forma remota pueden ser códigos

de autorización de transacciones virtuales (de un solo uso) o tokens RFID virtuales que utilizan deliberadamente un formato de UID no estándar para evitar posibles conflictos con los valores de UID reales que se utilizan al iniciar la recarga con un paso de tarjeta.

También, en el caso que se verá después de identificadores superiores o de grupo, se puede utilizar otro identificador superior con otro formato cuando hay una cuenta central en la que unos usuarios tienen permiso para detener las recargas de otros usuarios.

Mientras cumpla un formato de *CiString20Type* (cadena de texto de tamaño máximo 20 caracteres) se puede enviar cualquier cosa siempre que se trate de un identificador significativo (que identifique al usuario que inicia o finaliza carga).

Esta parte de la autorización es la que puede estar más comprometida y es en la que se tratará de fortalecer su seguridad a lo largo de este trabajo. Además, se recomienda la representación de estos identificadores en hexadecimal, como ya se mencionó antes.

4.1.5. Identificadores superiores

Un CSMS tiene la capacidad de tratar un conjunto de identificadores como un grupo, lo que permite que cualquier identificador de ese grupo inicie una transacción y que el mismo token u otro token del mismo grupo pueda detenerla. Esto es compatible con los casos de uso comunes de familias o empresas con múltiples conductores para una flota de vehículos compartidos que usan en una sola cuenta de contrato de recarga.

Se agrupan con fines de autorización especificando un identificador de grupo superior. Se considera que dos identificadores están en el mismo grupo si disponen de una etiqueta superior que coincide en ambos.

Se trata del mismo caso que un identificador único de un usuario por lo que, al fortalecer la seguridad de este, la protección frente a posibles robos del identificador aplica también en este caso.

4.1.6. Operaciones iniciadas por el punto de recarga

En este apartado se tratarán los modos de comunicación entre punto de recarga y CSMS más relevantes.

4.1.6.1. Authorize (autorizar)

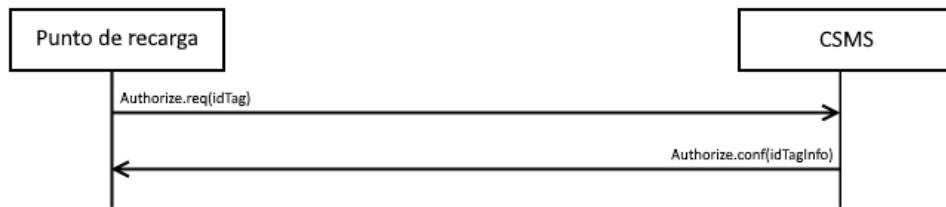


Figura 4.4: Diagrama de Authorize

Antes de que el propietario de un vehículo eléctrico sea capaz de iniciar o detener la carga, el punto de recarga tiene que autorizar la operación. Este solo debería suministrar energía previa autorización. Al detener una transacción, el punto de recarga sólo debería enviar un paquete de autorización cuando el identificador utilizado para detener la transacción es diferente del que inició la transacción.

Un punto de recarga podría autorizar al identificador localmente sin involucrar al CSMS, como se describe en *Modos de autorización local y funcionamiento sin conexión* (4.1.2). Si una etiqueta de identificación presentada por el usuario no está en la lista de autorización local o en la memoria caché de autorización el punto de recarga debería enviar una solicitud de autorización al CSMS para solicitar autorización. Si, en caso contrario, está presente en la lista de autorización local o en la memoria caché de autorización, el punto de recarga simplemente podría enviar una solicitud de autorización al CSMS. Si el punto de recarga dispone de una caché de autorización, al recibir una confirmación de autorización, el punto de recarga debe actualizar la entrada de caché dependiendo de si esta tiene permiso o no. En el caso que se trata esta configuración está desactivada.

Al recibir una solicitud de autorización, el CSMS debería responder con una confirmación de autorización. Esta última debe indicar si el CSMS acepta o no la etiqueta de identificación. Si el CSMS acepta esta etiqueta, la confirmación podría

incluir una etiqueta de identificación superior y debe incluir un valor de estado de autorización que indique la aceptación o el motivo del rechazo.

4.1.6.2. BootNotificacion (notificación de arranque)

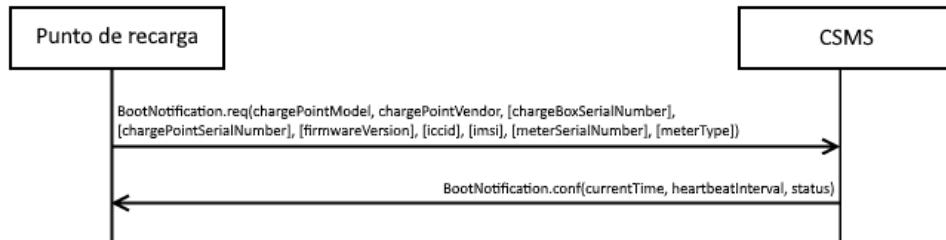


Figura 4.5: Diagrama de BootNotification

Después de la puesta en marcha un punto de recarga debe enviar una solicitud al CSMS con información sobre su configuración (marca, proveedor, etc.). El CSMS debería responder para indicar si lo acepta en el sistema o no.

El punto de recarga debería enviar una solicitud *BootNotification* cada vez que arranca o reinicia. Entre el encendido/reinicio físico y la finalización exitosa de una *BootNotification*, donde el CSMS devuelve o aceptado o pendiente, el punto de recarga no enviará ninguna solicitud distinta al CSMS. Esto incluye los mensajes antiguos todavía almacenados en la caché del punto de recarga.

Cuando el CSMS responde al *BootNotification* con el estado aceptado, el punto de recarga ajustará el intervalo de Heartbeat (que consisten en avisos periódicos al CSMS de que sigue en funcionamiento y con conexión) de acuerdo con el intervalo que recibe en la confirmación y se recomienda sincronizar su reloj interno con la hora actual del CSMS suministrado. Si el CSMS responde a la solicitud *BootNotification* algo que no sea del valor aceptado, el valor del campo de intervalo indica el tiempo de espera mínimo antes de enviar una próxima solicitud *BootNotification*. Si ese valor de intervalo es cero, el punto de recarga lo elige por su cuenta, para evitar inundar el CSMS con estas solicitudes. Un punto de recarga debe enviar una solicitud *BootNotification* antes de que se supere este tiempo a menos que el CSMS le solicite hacerlo con un mediante una solicitud llamada *TriggerMessage*.

Si el CSMS devuelve el estado rechazado, el punto de recarga no enviará ningún mensaje OCPP al CSMS hasta que haya expirado el mencionado intervalo de

reintento. Durante este, es posible que ya no se pueda acceder al punto de recarga desde el CSMS. Este podría cerrar su canal de comunicación o apagar el hardware de comunicación, por ejemplo, para liberar recursos del sistema. Si el estado es rechazado, el punto de recarga no debe responder a ningún mensaje iniciado por el CSMS ni este último debe iniciar ninguna comunicación.

El CSMS podría devolver también un estado pendiente de registro para indicar que se busca recuperar o configurar algún parámetro en el punto de recarga antes de que el CSMS acepte el punto de recarga. Si este devuelve el estado pendiente de registro, el canal de comunicación no debería ser cerrado ni por el punto de recarga ni por el CSMS. El punto de recarga debería responder a estos mensajes y no debería enviar mensajes de solicitud al CSMS a menos que, como se dice anteriormente, este le haya dado instrucciones para hacerlo con una solicitud *TriggerMessage*.

En este estado pendiente de registro, el CSMS no puede iniciar ni una solicitud *RemoteStartTransaction* ni una *RemoteStopTransaction*. Sí debería aceptar transacciones autorizadas mediante caché, aunque estas puedan no entregarse al sistema central. Igualmente, en el caso que se estudia en este trabajo no va a aplicar.

4.1.6.3. Heartbeat (latido)



Figura 4.6: Diagrama de Heartbeat

Para que el CSMS sepa que un punto de recarga se mantiene activo y conectado, un punto de recarga deberá enviar una solicitud *Heartbeat* después de un intervalo de tiempo configurable.

Al recibir una solicitud *Heartbeat*, el CSMS debería responder con una confirmación *Heartbeat*. La confirmación contendrá la hora actual del CSMS, la cual se recomienda utilizar por parte del punto de recarga para sincronizar su reloj interno.

El punto de recarga podría omitir el envío de una solicitud *Heartbeat* cuando se ha enviado otra solicitud al CSMS dentro del intervalo de *Heartbeat* configurado.

Esto implica que un CSMS debería asumir la disponibilidad de un punto de recarga siempre que haya recibido una solicitud, de la misma manera que lo habría hecho cuando recibió una solicitud *Heartbeat*.

Con JSON sobre WebSocket el envío de este tipo de paquetes no es obligatorio. Sin embargo, por sincronización horaria, se recomienda enviar al menos uno cada día.

4.1.6.4. MeterValues (valores del medidor)

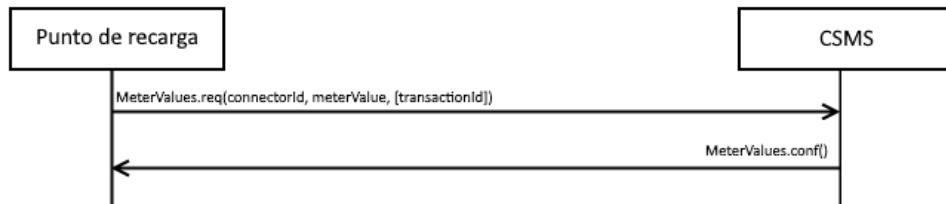


Figura 4.7: Diagrama de MeterValues

Un punto de recarga debe muestrear el medidor de energía u otro tipo de hardware sensor o transductor para proporcionar algún tipo de información adicional sobre los valores de este. Depende del punto de recarga la decisión de cuándo enviará los valores del medidor. Esto se puede configurar usando una solicitud llamada *ChangeConfiguration* para configurar los intervalos de adquisición de datos y especificar los datos que se adquirirán y reportarán.

El punto de recarga debe enviar una solicitud *MeterValues* para descargar los valores de contadores. Debe contener el id del conector del que se tomaron las muestras, el id de la transacción a la que se relacionan, si corresponde, y los elementos de valores de *MeterValues*.

En primer lugar, si el *ConnectorId* es 0, el mensaje se asocia a todo el punto de recarga. Si el *ConnectorId* es 0 y la magnitud está relacionada con la energía, esta muestra debe tomarse del medidor de energía principal.

Por otro lado, si no hay una transacción en curso o si los valores se toman del medidor principal se puede omitir el *TransactionId*.

Finalmente, los valores del *MeterValues*, cada uno de los cuales representa un conjunto de uno o más valores de datos recogidos en un momento determinado.

Cada elemento *MeterValues* contiene una marca de tiempo y un conjunto de uno o más elemento de valor de muestreo, todos capturados en el mismo momento. Cada elemento de valor muestreado contiene un único dato de valor. La naturaleza de cada valor muestreado está determinada por los opcionales *magnitud*, *contexto*, *ubicación*, *unidad*, *fase*, y el *formato de campos*.

El campo opcional *magnitud* especifica el tipo de valor que se mide/informa.

El campo opcional *contexto* especifica el motivo/evento que desencadena la lectura del medidor.

El campo opcional *ubicación* especifica dónde se toma la medición (p. ej., entrada, salida).

El campo opcional *fase* especifica a qué fase o fases de la instalación eléctrica se aplica el valor. El punto de recarga debería informar de todos los valores dependientes del número de fase desde el punto de vista del medidor de energía (o la conexión a la red cuando esté ausente). Igualmente, este campo no es aplicable a todos los tipos de medidas. Por otro lado, hay están dos valores disponibles que estrictamente hablando no se refieren a valores medidos en ningún momento puntual. Estos se refieren a la cantidad máxima de corriente/potencia que se ofrece al EV y están destinados para su uso en aplicaciones de carga inteligente.

Para la información de rotación de fase de un conector individual, el CSMS puede consultar la configuración del mismo en el punto de recarga con la opción *ConnectorPhaseRotation* mediante un paquete llamado *GetConfiguration*. El punto de recarga debe informar de la rotación de fases con respecto a la conexión a la red. Los valores configurables por conector son *NotApplicable*, *Unknown*, *RST*, *RTS*, *SRT*, *STR*, *TRS* y *TSR*.

El campo experimental *formato* especifica si los datos se representan en la forma normal (predeterminada) como un valor numérico simple (*crudo*), o como *datos firmados*, un bloque de datos binarios con firma digital opaca, representado como datos hexadecimales. Este campo experimental podría quedar obsoleto y más adelante eliminado en versiones posteriores cuando se proporcione una alternativa de solución más madura.

Para mantener la compatibilidad con versiones anteriores, los valores predeterminados de todos los camposopcionales en un elemento de valor muestreado son tales que un valor sin ningún campo adicional se interpretará como una lectura de registro de energía de importación activa en unidades de Wh (wattos hora).

Es probable que el CSMS haga alguna comprobación sobre los datos obtenidos de una solicitud *MeterValues*. El resultado de tales comprobaciones no debe generar que el CSMS no responda con una confirmación *MeterValues*. No responder correctamente hará que el punto de recarga vuelva a intentar el mismo mensaje.

4.1.6.5. StartTransaction (iniciar transacción)

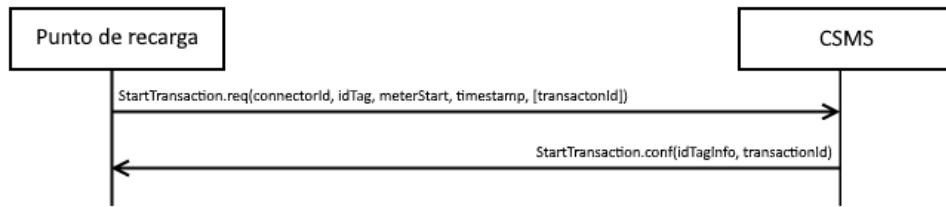


Figura 4.8: Diagrama de StartTransaction

El punto de recarga debe enviar una solicitud *StartTransaction* al CSMS para informar sobre el inicio de una transacción. Si esta transacción se corresponde con una reserva, la solicitud *StartTransaction* tendrá que contener el identificador de la reserva.

Al recibir una solicitud *StartTransaction*, el CSMS deberá de responder con una confirmación *StartTransaction*. Este mensaje de confirmación debe incluir una identificación de transacción y un valor de estado de autorización.

El CSMS debería verificar la validez del identificador en la solicitud *StartTransaction* recibida, porque el identificador podría haber sido autorizado localmente por la caché de autorización existente en el punto de recarga utilizando información desactualizada. El identificado, por ejemplo, puede haber sido bloqueado en el CSMS en el intervalo en la última conexión del punto de recarga con él y en la llegada del *StartTransaction*. Tras recibir un *StartTransaction* debe actualizar la entrada de caché si es que ese identificador no está en la misma. En cualquier caso, en este trabajo no va a aplicarse esta configuración.

Es probable que el CSMS haga alguna comprobación sobre los datos obtenidos de una solicitud *StartTransaction*. El resultado de tales comprobaciones no debe generar que el CSMS no responda con una confirmación *StartTransaction*. No responder correctamente hará que el punto de recarga vuelva a intentar el mismo mensaje.

4.1.6.6. StatusNotification (notificación de estado)

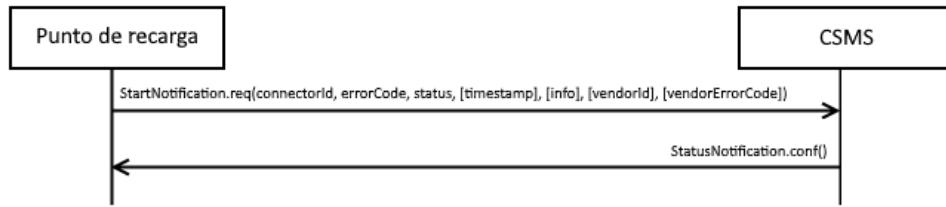


Figura 4.9: Diagrama de StatusNotification

Un punto de recarga envía una notificación al CSMS para informarle sobre un cambio de estado o un error dentro del punto de recarga. La siguiente tabla muestra todos los posibles estados con los cambios de un estado anterior (columna izquierda) a un estado nuevo (fila superior) en el que un punto de recarga puede enviar una solicitud *StatusNotification* al CSMS.

Los posibles estados del punto de recarga y su denominación en la tabla de estados son:

1. Available (A, 1): disponible.
2. Preparing (B, 2): preparando.
3. Charging (C, 3): cargando.
4. Suspended EV (D, 4): EV suspendido.
5. Suspended EVSE (E, 5): EVSE suspendido.
6. Finishing (F, 6): Finalizando.
7. Reserved (G, 7): Reservado.
8. Unavailable (H, 8): No disponible.
9. Faulted (I, 9): Fallado.

Tabla 4.1: Estados del punto de recarga y su tabla de flujo

	1	2	3	4	5	6		7	8	9
A	-	A2	A3	A4	A5	-		A7	A8	A9
B	B1	-	B3	B4	B5	-		-	-	B9
C	C1	-	-	C4	C5	C6		-	C8	C9

D	D1	-	D3	-	D5	D6		-	D8	D9
E	E1	-	E3	E4	-	E6		-	E8	E9
F	F1	F2	-	-	-	-		-	F8	F9
G	G1	G2	-	-	-	-		-	G8	G9
H	H1	H2	H3	H4	H5	-		-	-	H9
I	I1	I2	I3	I4	I5	I6		I7	I8	-

La siguiente tabla describe los eventos que pueden llevar a un cambio de estado:

Tabla 4.2: Eventos que pueden llevar a cambios de estado

-	No es posible
A2	Se inicia el uso (por ejemplo, se enchufa el vehículo, se pasa una etiqueta de identificación, se recibe una solicitud de RemoteStartTransaction...)
A3	Podría ser posible en un punto de recarga sin la obligación de autorizarse activa
A4	Similar al A3 pero el EV no comienza a cargar
A5	Similar al A3 pero el EVSE no comienza a cargar
A7	Se recibe un mensaje <i>Reserve Now</i> (reservar ahora)
A8	Se recibe un mensaje <i>Change Availability</i> (cambio de disponibilidad) que marca el conector como <i>Unavailable</i>
A9	Se detecta un fallo que impide posteriores operaciones de carga
B1	Se finaliza el uso previsto (por ejemplo, se desenchufa el vehículo, se pasa por segunda vez una etiqueta de identificación, se agota el tiempo de espera hasta una acción del usuario...)
B3	Se cumplen todos los requisitos previos para iniciar la carga y comienza el proceso
B4	Se cumplen todos los requisitos previos para la carga, pero el EV no comienza a cargar
B5	Se cumplen todos los requisitos previos para la carga, pero el EVSE no comienza a cargar
B9	Se detecta un fallo que impide posteriores operaciones de carga
C1	La sesión de carga finaliza sin haberse requerido ninguna acción por parte del usuario (por ejemplo, se quitó la manguera en el lado del EV)

C4	La carga se detiene cuando lo solicita el EV
C5	La carga se detiene cuando lo solicita el EVSE (por ejemplo, restricción de carga inteligente, la transacción es invalidada por una solicitud AuthorizationStatus en una confirmación StartTransaction)
C6	La sesión de carga es detenida por el usuario o un RemoteStopTransaction y se requiere una acción adicional del usuario consistente en quitar el cable
C8	La sesión de carga finaliza, no se requiere ninguna acción del usuario y el conector está programado para ponerse en el estado <i>Unavailable</i>
C9	Se detecta un fallo que impide posteriores operaciones de carga
D1	La sesión de carga finaliza sin haberse requerido ninguna acción por parte del usuario (por ejemplo, se quitó la manguera en el lado del EV)
D3	La carga se reanuda a petición del EV
D5	EVSE suspende la carga
D6	La sesión de carga se detiene y se requiere más acción del usuario (quitar el cable)
D8	La sesión de carga finaliza, no se requiere ninguna acción del usuario y el conector está programado para ponerse en el estado <i>Unavailable</i>
D9	Se detecta un fallo que impide posteriores operaciones de carga
E1	La sesión de carga finaliza sin haberse requerido ninguna acción por parte del usuario (por ejemplo, se quitó la manguera en el lado del EV)
E3	La carga se reanuda porque se levanta la petición EVSE
E4	Se levanta la petición EVSE pero el EV no comienza a cargar
E6	La sesión de carga se detiene y se requiere más acción del usuario (quitar el cable)
E8	La sesión de carga finaliza, no se requiere ninguna acción del usuario y el conector está programado para ponerse en el estado <i>Unavailable</i>
E9	Se detecta un fallo que impide posteriores operaciones de carga
F1	Completadas todas las acciones del usuario
F2	El usuario reinicia la sesión de carga (por ejemplo, se vuelve a enchufar el vehículo, se vuelve a pasar una etiqueta de identificación...)
F8	Se completan todas las acciones del usuario y el conector está programado para ponerse en el estado <i>Unavailable</i>
F9	Se detecta un fallo que impide posteriores operaciones de carga

G1	La reserva caduca o se recibe un mensaje <i>Cancel Reservation</i> (cancelación de reserva)
G2	Se presenta la identidad de la reserva
G8	La reserva caduca o se recibe un mensaje <i>Cancel Reservation</i> (cancelación de reserva) y el conector está programado para ponerse en el estado <i>Unavailable</i>
G9	Se detecta un fallo que impide posteriores operaciones de carga
H1	El conector se configura como <i>Disponible</i> después de que llegase un mensaje <i>Change Availability</i> (cambiar disponibilidad)
H2	El conector se configura como <i>Disponible</i> después de que el usuario haya interactuado con el punto de recarga
H3	El conector se configura como <i>Disponible</i> y no se requiere ninguna acción del usuario para comenzar a cargar
H4	Similar a H3 pero el EV no comienza a cargar
H5	Similar a H3 pero el EVSE no comienza a cargar
H9	Se detecta un fallo que impide posteriores operaciones de carga
I1-I8	El fallo se resuelve y el estado vuelve al estado previo al fallo

Estas tablas solo aplican cuando el *ConnectorId* es mayor que 0. Para el *ConnectorId* 0, que se refiere al general del punto, solo están disponibles los estados *Available*, *Unavailable*, *Faulted*. El estado de *ConnectorId* 0 no tiene conexión directa con el estado de los conectores individuales mayores que 0.

Por otro lado, si tanto el EV como el EVSE suspenden la carga, el estado *SuspendedEVSE* tendrá prioridad sobre el estado *SuspendedEV*.

Cuando un punto de recarga o un conector cambian su estado a *Unavailable* por una solicitud *ChangeAvailability*, el estado *Unavailable* debería ser persistente en todos los reinicios. El punto de recarga puede utilizar el estado *Unavailable* internamente para otros fines (por ejemplo, mientras se actualiza el firmware)

Ya que el estado *Occupied* se ha subdividido en cinco nuevos estados (*Preparing*, *Charging*, *SuspendedEV*, *SuspendedEVSE* y *Finishing*), se envían más solicitudes *StatusNotification*. Estas se enviarán desde el punto de recarga al CSMS. Por ejemplo, cuando se inicia una transacción, el estado del conector cambiaría sucesivamente

de *Preparing* a *Charging* con un corto *SuspendedEV* y/o *SuspendedEVSE* en el medio, con una duración de en torno a un par de segundos.

Para limitar el número de cambios de estado, el punto de recarga puede omitir el envío de una solicitud *StatusNotification* si estuvo activo menos tiempo del definido en la clave de configuración opcional *MinimumStatusDuration* (duración mínima del estado). De esta forma, un punto de recarga puede optar por no enviar algunas solicitudes *StatusNotification*. Por otro lado, un fabricante de puntos de recarga puede haber implementado una duración de estado mínima (retardo) para ciertas transiciones de estado separadas de la opción *MinimumStatusDuration*. El tiempo establecido en *MinimumStatusDuration* se agregaría a este retraso predeterminado. Ajustar *MinimumStatusDuration* a cero no anula la duración de estado mínima predeterminada del fabricante. Establecer un valor alto de este parámetro podría retrasar todas las notificaciones de estado, ya que el punto de recarga solo lo mandaría después de que pasase ese tiempo.

El punto de recarga puede enviar una solicitud *StatusNotification* para informar al CSMS de algunas condiciones que producen unfallo. Cuando el campo estado no está *Faulted* esa condición debe considerarse una advertencia, ya que las operaciones de carga aún son posibles.

El *ChargePointErrorCode* (código de error de punto de carga *EVCommunicationError*) solo deberá usarse con el estado *Preparing*, *SuspendedEV*, *SuspendedEVSE* y *Finishing* y se tratará como si fuese una advertencia.

Cuando un punto de recarga está configurado con *StopTransactionOnEVSideDisconnect* (detener la transacción tras desconexión del lado EV) configurado a falso, se está realizando una carga y esta se desconecta del lado del EV, el estado *SuspendedEV* debería enviarse al CSMS mediante una solicitud *StatusNotification*, con el campo *errorCode* establecido en *NoError*. El punto de recarga entonces tiene que añadir información adicional en el campo *info*, notificando al CSMS con el motivo de la suspensión de la recarga, que sería *EV side disconnected* (lado EV desconectado). La transacción actual no se detiene.

Sin embargo, cuando un punto de recarga está configurado con *StopTransactionOnEVSideDisconnect* fijado a verdadero, se está ejecutando una carga y el EV se desconecta del lado del EV, se debería enviar al CSMS una solicitud *StatusNotification* con el estado *Finishing*, con el campo *errorCode* establecido en *NoError*. El punto de recarga debería añadir información adicional en el campo *info*, notificando

al CSMS con el motivo de la suspensión de la recarga, que sería *EV side disconnected* (lado EV desconectado). La transacción actual no se detiene.

Cuando un punto de recarga se conecta a un CSMS después de haber sido desconectado, actualiza al CSMS sobre su estado de acuerdo a las siguientes reglas:

- El punto de recarga debería enviar una solicitud *StatusNotification* con su estado actual si es que este cambió mientras el punto de recarga estaba desconectado.
- El punto de recarga puede enviar una solicitud *StatusNotification* para informar de un error que sucedió cuando el punto de recarga estaba desconectado.
- El punto de recarga no debe enviar una solicitud *StatusNotification* para eventos de cambio de estado históricos que ocurrieron mientras el punto de recarga estaba fuera de línea y que no informan al CSMS de errores del propio punto de recarga o de su estado actual.
- Las solicitudes *StatusNotification* deben enviarse en el orden en el que ocurrieron los eventos que se describen en ellos.

Al recibir una solicitud *StatusNotification* el CSMS debería responder con una confirmación *StatusNotification*

4.1.6.7. StopTransaction (detener transacción)

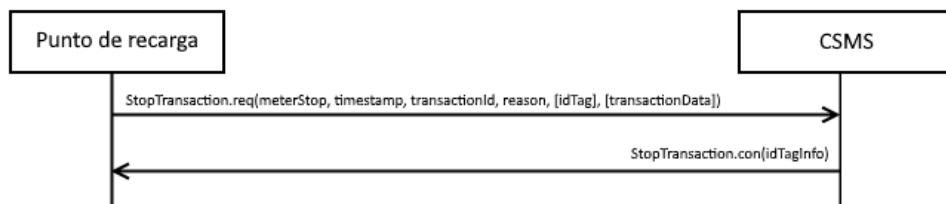


Figura 4.10: Diagrama de StopTransaction

Cuando se detiene una carga, el punto de recarga debe enviar una solicitud *StopTransaction*, notificando al CSMS que esta se ha detenido.

A una solicitud *StopTransaction* puede contener un opcional *TransactionData* (datos de la transacción) para proporcionar más detalles sobre el uso de transacciones. Este elemento es un contenedor para cualquier número de *MeterValues*, uti-

lizando la misma estructura de datos que los elementos *meterValue* de la solicitud *MeterValues*.

Al recibir una solicitud *StopTransaction*, el CSMS debería responder con una confirmación *StopTransaction*.

El CSMS no puede evitar que una transacción se detenga. Únicamente puede informar al punto de recarga que ha recibido la solicitud *StopTransaction* y puede enviar información sobre la etiqueta de identificación utilizada para detener la transacción. Esta información se utilizará para actualizar la caché de autorización, si se implementa. En este trabajo no se va a implementar.

La etiqueta de identificación en la solicitud puede omitirse cuando el punto de recarga necesita detener la transacción. Por ejemplo, cuando se solicita el reinicio del punto de recarga.

Si una transacción finaliza de forma normal, el elemento *Razón* se puede omitir y debería asumirse como *Local*. Si la transacción no finaliza normalmente, este debe establecerse en un valor correcto. Como parte de la finalización normal de la transacción, el punto de recarga debería desbloquear el cable si es que este no está conectado permanentemente.

El punto de recarga puede detener una transacción en curso cuando se desconecta el cable del vehículo eléctrico. Si esta funcionalidad es compatible, es informada y controlada por la clave de configuración *StopTransactionOnEVSideDisconnect*. Si se establece en falso, la transacción no se debe detener cuando el cable se desconecta del EV. Si se vuelve a conectar el EV, se permitiría nuevamente la transferencia de energía. En este caso, no hay ningún tipo de mecanismo para evitar que otros vehículos eléctricos distintos se carguen y desconecten durante la misma transacción en curso. Con *UnlockConnectorOnEVSideDisconnect* ajustado a falso, el conector debería permanecer bloqueado en el punto de recarga hasta que el usuario detenga la recarga. En caso de que *StopTransactionOnEVSideDisconnect* sea falso, tiene prioridad sobre *UnlockConnectorOnEVSideDisconnect*. En otras palabras, los cables siempre permanecen bloqueados cuando el cable está desconectado en el lado EV al estar fijado *StopTransactionOnEVSideDisconnect* en falso. Configurando *StopTransactionOnEVSideDisconnect* a verdadero, la transacción se debería detener cuando el cable se desconecte del EV. Si se vuelve a conectar el EV, no se permitiría la transferencia de energía hasta que se detenga la transacción y se iniciará una nueva transacción. Si *UnlockConnectorOnEVSideDisconnect* se configura a verdadero, también se desbloqueará el conector del punto de recarga. En este trabajo,

StopTransactionOnEVSideDisconnect se configurará a verdadero y *UnlockConnectorOnEVSideDisconnect* a falso. Esto evitará que un usuario no autorizado libere un vehículo conectado al punto de recarga para posteriormente conectar el suyo y cargar sin permiso.

Es probable que el CSMS aplique controles de cordura a los datos contenidos en una solicitud *StopTransaction* recibida. El resultado de tales verificaciones de cordura no puede provocar que el CSMS no responda con una confirmación *StopTransaction*. No responder con ella solo hará que el punto de recarga vuelva a intentar el mismo mensaje.

Si el punto de recarga ha implementado un caché de autorización, luego de recibir una solicitud *StopTransaction*, el punto de recarga debe actualizar la entrada de caché, si la etiqueta de identificación no está en la lista de autorizaciones locales, con el valor *IdTagInfo* de la confirmación como se describe en la caché de autorización. En este caso no aplica.

4.1.7. Operaciones iniciadas por el CSMS

4.1.7.1. ChangeConfiguration (cambiar configuración)

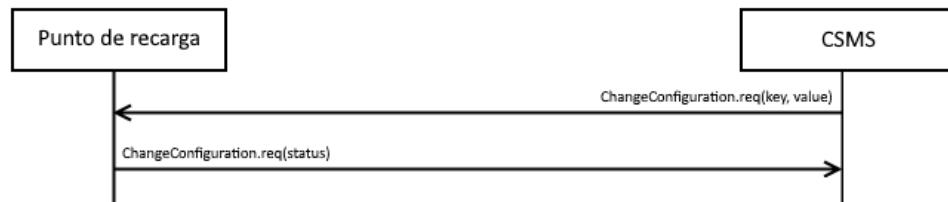


Figura 4.11: Diagrama de ChangeConfiguration

El CSMS puede hacer una solicitud a un punto de recarga para cambiar los parámetros de configuración. Para lograr esto, el CSMS debe enviar una solicitud llamada *ChangeConfiguration*. Esta solicitud contiene un par *key-value*, donde *key* (clave) es el nombre de la configuración que se va a cambiar y *value* (valor) contiene el nuevo valor para la configuración.

Al recibir una solicitud *ChangeConfiguration* el punto de recarga deberá enviar una confirmación *CambiarConfiguración* indicando si fue capaz de ejecutar el cambio. El contenido de *key* y *valor* no está predefinido. Si *key* no corresponde a un

ajuste de configuración compatible con el punto de recarga, este responderá con un estado *NotSupported* (no compatible). Si por el contrario el cambio se ejecutó de manera exitosa se responderá con un estado *Accepted* (aceptado). Si el cambio se ejecutó correctamente, pero es necesario reiniciar el punto de recarga para aplicarlo, la confirmación contendrá el estado *RebootRequired* (reinicio requerido). En caso de no establecer la nueva configuración, el punto de recarga deberá responder con el estado *Rejected* (rechazado).

4.1.7.2. ClearCache (limpiar caché)

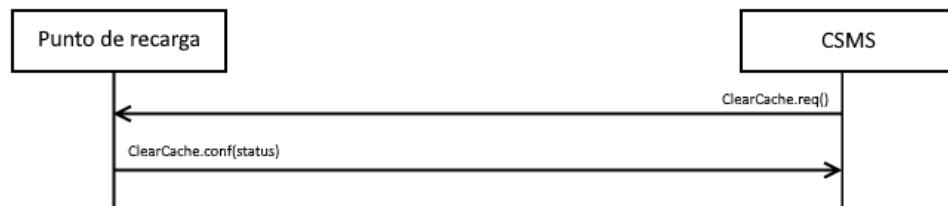


Figura 4.12: Diagrama de ClearCache

El CSMS puede solicitar a un punto de recarga que borre su caché de autorización. El CSMS tiene que enviar una solicitud *ClearCache* para borrar la memoria de la caché de autorización del punto de recarga. El punto de recarga tendrá que responder con una confirmación *ClearCache*, la cual debe indicar si el punto de recarga pudo borrar esta caché de autorización. En este trabajo no será necesario al no estar configurada.

4.1.7.3. GetConfiguration (obtener configuración)

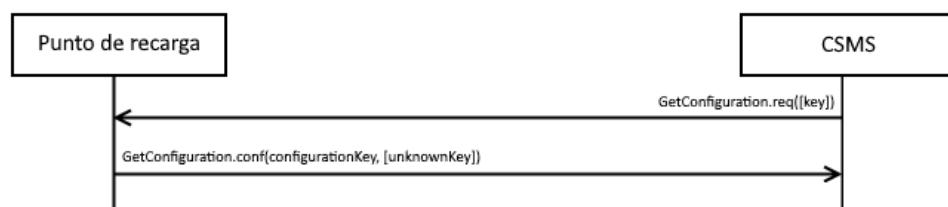


Figura 4.13: Diagrama de GetConfiguration

Para recuperar el valor de los ajustes de configuración, el CSMS enviará una solicitud *GetConfiguration* al punto de recarga. Si la lista de claves en la PDU está vacía o falta (es opcional), el punto de recarga debe devolver una lista de todos los ajustes de configuración en la confirmación *GetConfiguration*. De lo contrario, el punto de recarga deberá devolver una lista de claves reconocidas y sus valores correspondientes y estado de solo lectura. Las claves no reconocidas deberían colocarse en la confirmación del punto de recarga como parte del elemento opcional de la lista de claves desconocidas.

El punto de recarga podría limitar el número de claves de configuración solicitadas en una sola solicitud. Este máximo se podría recuperar leyendo la clave de configuración *GetConfigurationMaxKeys*.

4.1.7.4. RemoteStartTransaction (inicio de recarga remoto)

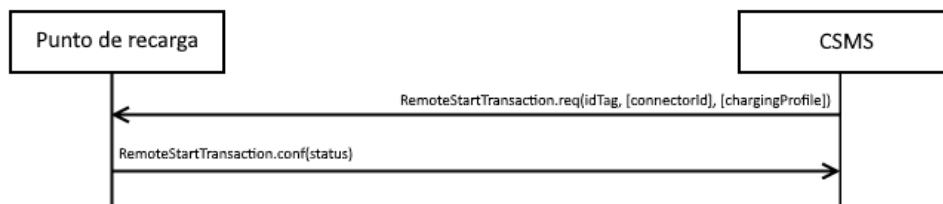


Figura 4.14: Diagrama de RemoteStartTransaction

El CSMS puede solicitar un punto de recarga para iniciar una transacción enviando una solicitud *RemoteStartTransaction*. Tras la recepción, el punto de recarga deberá responder con una confirmación *RemoteStartTransaction* y un estado que indica si puede iniciar una transacción o no.

El funcionamiento del mensaje de solicitud *RemoteStartTransaction* depende del valor de la clave de configuración *AuthorizeRemoteTxRequestsclave* de configuración en el punto de recarga.

Si el valor de esta clave *AuthorizeRemoteTxRequests* es verdadero, el punto de recarga debería comportarse como si respondiera a una acción local en el punto de recarga para iniciar una transacción con la etiqueta de identificación proporcionada en el mensaje de solicitud de *RemoteStartTransaction*. Esto significa por tanto que el punto de recarga primero intentará autorizar la etiqueta de identificación, utilizando o la lista de autorizaciones locales, o la caché de autorización y/o una

solicitud *Authorize*. Una transacción solo se iniciará después de que se haya obtenido esta autorización. Por otro lado, si el valor de esta clave es falso, el punto de recarga debe intentar inmediatamente iniciar una transacción para la etiqueta de identificación proporcionada en el mensaje de solicitud de *RemoteStartTransaction*. Tenga en cuenta que una vez iniciada la transacción, el punto de recarga le enviará un *StartTransaction* al CSMS, y el CSMS verificará el estado de autorización de la etiqueta de identificación al procesar esta solicitud de *StartTransaction*.

Estos son los casos más habituales de *RemoteStartTransaction*:

- Permitir que un operador de CPO ayude a un conductor de EV que tiene problemas para iniciar una transacción.
- Habilitar aplicaciones móviles para controlar transacciones de cobro a través del CSMS.
- Habilitar el uso de SMS para controlar transacciones de cobro a través del CSMS.

Las solicitudes *RemoteStartTransaction* deben contener un identificador (*idTag*) que el punto de recarga debe utilizar, si puede iniciar una transacción, para enviar una solicitud *StartTransaction* al CSMS. La transacción se inicia de la misma manera que se describe en *StartTransaction*. Las solicitudes *RemoteStartTransaction* pueden contener una identificación de conector si la transacción se va a iniciar en un conector específico. Cuando no se proporciona una identificación de conector, el punto de recarga tiene el control de la selección del mismo. Un punto de recarga podría rechazar un *RemoteStartTransaction* sin una identificación del conector.

4.1.7.5. RemoteStopTransaction (detención de recarga remoto)

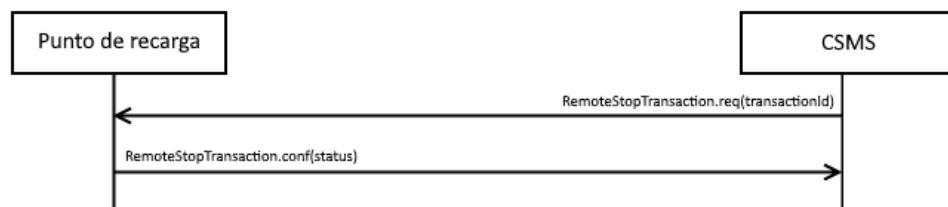


Figura 4.15: Diagrama de RemoteStopTransaction

El CSMS puede solicitar a un punto de recarga que detenga una transacción enviando una solicitud *RemoteStopTransaction* al punto de recarga con el identificador de la transacción. El punto de recarga debería responder con una confirmación *RemoteStopTransaction* para indicar si está capacitado para detener la transacción.

Esta solicitud remota para detener una transacción es igual a una acción local para detener una transacción. Por tanto, si la transacción es detenida, el punto de recarga enviará una solicitud *StopTransaction* y, en su caso, desbloquear el conector.

Estos son los casos más habituales de *RemoteStopTransaction*:

- Permitir que un operador de CPO ayude a un conductor de EV que tiene problemas para detener una transacción.
- Habilitar aplicaciones móviles para controlar transacciones de cobro a través del CSMS.

4.1.7.6. Reset (reiniciar)

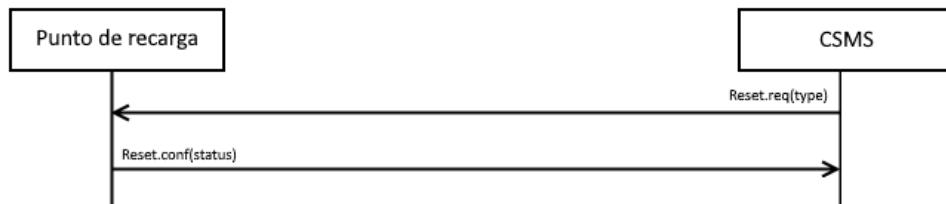


Figura 4.16: Diagrama de Reset

El CSMS debería enviar una solicitud *Reset* para solicitar que un punto de recarga se reinicie. El CSMS puede solicitar un restablecimiento completo o parcial. Al recibir una solicitud *Reset*, el punto de recarga debería responder con una confirmación *Reset*. La confirmación debe incluir si el punto de recarga acepta y, por tanto, intenta el reinicio.

Al recibir un restablecimiento parcial, el punto de recarga debería volver a un estado en el que se comporte como si acabara de arrancar. Si alguna transacción está en progreso, debería terminarse normalmente, antes del reinicio, como en un *StopTransaction*.

Al recibir un restablecimiento completo, el punto de recarga debería intentar finalizar cualquier transacción en curso normalmente como en *StopTransaction* y luego realizar un reinicio.

4.1.7.7. **UnlockConnector** (desbloqueo de conector)

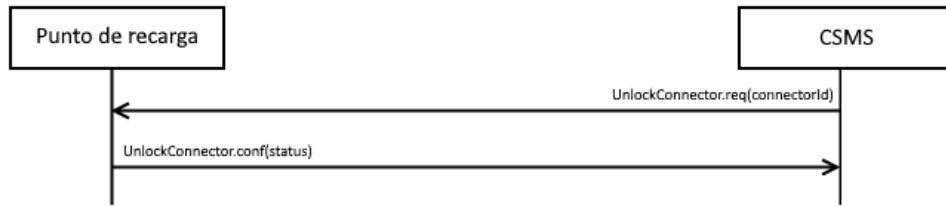


Figura 4.17: Diagrama de UnlockConnector

El CSMS puede solicitar a un punto de recarga desbloquear un conector. Para ello, el punto de recarga debería enviar una solicitud *UnlockConnector*

El objetivo de este mensaje es el de ayudar a los conductores de EV que tienen problemas para desconectar el cable del punto de carga en caso de algún tipo de mal no esperado funcionamiento de la retención del cable del conector. Cuando un conductor de un EV llama al *help-desk* de CPO, un operador podría activar manualmente el envío de una solicitud *UnlockConnector* al punto de recarga, obligando a un nuevo intento de desbloqueo del conector. Si todo va según lo previsto esta vez el conector se desbloqueará y el conductor del vehículo eléctrico podrá desconectar el cable y marcharse.

Al recibir una solicitud *UnlockConnector*, el punto de recarga responderá con una confirmación *UnlockConnector*. La confirmación debe indicar si el punto de recarga pudo desbloquear su conector.

Si existe una transacción en curso en el conector específico, el punto de recarga deberá finalizar la transacción igual que se hace en *StopTransaction*.

UnlockConnector está diseñado solo para desbloquear el bloqueo destinado a retener el cable en el conector, no para desbloquear la puerta de acceso al mismo.

Capítulo 5

Gestión de proyecto software

Realizar una simulación de la gestión del proyecto software desarrollo. La gestión simulará un proyecto real, realizado con las condiciones habituales del entorno empresarial. El objetivo del capítulo es plasmar los conocimientos adquiridos a lo largo de la titulación y no la forma en la cual se ha gestionado el Trabajo Fin de Máster. Extensión máxima de veinte páginas.

5.1. Alcance del proyecto

5.2. Presupuesto

A continuación se detalla un presupuesto estimado para el coste total de este proyecto.

5.2.0.1. Coste de personal

Tabla 5.1: Presupuesto de personal

Tarea	Perfil	Horas	Euros/Hora	Total
Búsqueda de información para el estado del arte	Jefe de Proyecto	60	40	2400 €
Desarrollo aplicación Android autenticación 2FA	Programador	60	20	1200 €
Desarrollo simulación NFC aleatorio	Programador	30	20	600 €
Pruebas	Ingeniero de Pruebas	15	30	450 €
Documentación	Jefe de Proyecto	120	40	4800 €
Total				9450 €

5.2.1. Coste del hardware

Para la realización de este proyecto se han utilizado los siguientes equipos:

1. Ordenador:

Placa base: ASUS X541UV

Procesador: Intel i7-6500U

RAM: 8 GB

Disco duro: 512GB SSD

Tarjeta gráfica: Nvidia GeForce 920MX

Monitor: 15,6"

- Precio (sin IVA): 354,55 €

1. Punto de recarga Alfen EVE MINI:

- Precio (sin IVA): 983,47 €

1. Smartphone:

Procesador: Snapdragon 665

RAM: 4 GB

Disco duro: 128GB

Monitor: 6,3"

- Precio (sin IVA): 132,23 €

5.2.2. Coste total

Tabla 5.2: Presupuesto total

Concepto	Coste (Euros)
Costes de personal	9450
Costes de hardware	1470,25
Subtotal	10920,25
IVA (21 %)	2293,25
Total Proyecto	13213,50 €

5.3. Plan de trabajo

5.3.1. Identificación de tareas

Para la realización de este proyecto se deben realizar varias tareas.

- Una revisión de la situación actual de las tecnologías que se van a utilizar (estado del arte). Servirá para conocer posibles vulnerabilidades sencillas de explotar y, además, varias de las posibles soluciones que se han implementado para ello.
- Conocer y probar algún método sencillo de explotación de esa vulnerabilidad.
- Pensar y reflexionar sobre posibles soluciones y formas de reducir la vulnerabilidad.
- Implementar mediante código o aplicaciones la solución o la simulación de la solución.

5.3.2. Estimación de tareas

Como ya se trata en el presupuesto, los tiempos de las tareas aproximadamente serían los siguientes:

1. El estado del arte llevaría un tiempo aproximado de 60 horas. Sería el jefe de proyecto el encargado de esta parte, ya que debería darle las pautas a los empleados de cuáles son los objetivos reales y los métodos para tratar las vulnerabilidades. Se divide en las siguientes subtareas:
 - a) Búsqueda de información.
 - b) Selección de información.
 - c) Lectura en detalle de los artículos y decisiones sobre ellos y actuaciones a seguir.
2. La implementación de los métodos llevaría unas 60 horas en el caso de la app de Android y 30 horas en la implementación NFC. Contienen las siguientes subtareas.
 - a) Diseño sencillo a mano de las pantallas y del flujo de la aplicación de Android.
 - b) Modificación de *Authorize* y *RemoteStartTransaction* y de la base de datos para que se cree la autorización en la misma.
 - c) Creación de servicio web que comunica el CSMS y la base de datos con la app.
 - d) Creación de app y flujo sin interactuar todavía con el servicio web.
 - e) Envío de información desde la app al servicio web para acceder como usuario.
 - f) Recepción de listado de autorizaciones pendientes desde el servicio web a la app.
 - g) Introducción de código en autorización y envío.
 - h) Creación de campos en la base de datos para la inserción de la tarjeta variable inicial, la final y la asociada a la carga.

- i) Cambios en Authorize, *RemoteStartTransaction* y *RemoteStopTransaction* para añadir las nuevas implementaciones para simular el paso y leer correctamente las tarjeta NFC variable.
 - j) Unión de ambas tecnologías.
3. Las pruebas llevarán un tiempo estimado de 15 horas:
- a) Prueba de concepto de robo de etiqueta RFID.
 - b) Pruebas autenticación 2FA.
 - c) Pruebas tarjeta NFC variable.
4. A lo largo del proyecto se irá realizando la redacción de la memoria.

El orden de las tareas, a excepción de la redacción de la memoria, es el indicado. En primer lugar, el estado del arte para, posteriormente, disponer de las ideas de planificación. Posteriormente se realizan las implementaciones del método de autenticación 2FA y la simulación de la tarjeta NFC variable.

El tiempo de realización total, contando algunos problemas o retrasos (tiempo de espera para continuar el proceso de desbloqueo del móvil, tiempo de espera para la llegada de algunos componentes para las pruebas...) suponiendo un trabajo diario de 2,5 horas (estimando la mitad de ellos para la redacción de la memoria a partir de la mitad de la tarea 1.c)) se ha repartido en unas 16 semanas.

Tabla 5.3: Estimación de tareas

Tarea	Días	Fecha de inicio	Fecha de fin
1. a)	8	9 de mayo	12 de mayo
1. b)	24	13 de mayo	24 de mayo
1. c)	16	25 de mayo	5 de junio
2. a)	2	14 de junio	15 de junio
2. b)	4	16 de junio	19 de junio
2. c)	10	20 de junio	29 de junio
2. d)	20	30 de junio	19 de julio
2. e)	2	20 de julio	21 de julio
2. f)	4	22 de julio	25 de julio
2. g)	6	26 de julio	31 de julio
2. h)	4	1 de agosto	4 de agosto
2. i)	18	5 de agosto	22 de agosto
2. j)	2	23 de agosto	24 de agosto
3. a)	8	6 de junio	13 de junio
3. b)	2	25 de agosto	26 de agosto
3. c)	2	27 de agosto	28 de agosto
4.	8	1 de junio	28 de agosto

5.3.3. Planificación de tareas

Se muestra, mediante un diagrama de Gantt, la planificación de las tareas. No se explican en el diagrama ningún tipo de relación ya que son consecutivas, exceptuando la memoria, que va a la vez que gran parte del desarrollo técnico del trabajo.

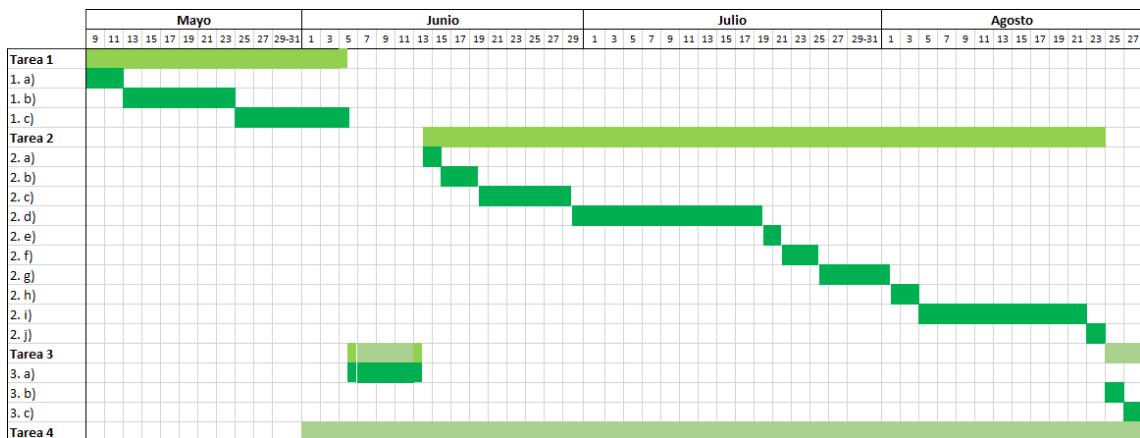


Figura 5.1: Diagrama de Gantt con la planificación de tareas

5.4. Gestión de recursos

Suponiendo una amortización total de cinco años para un ordenador portátil o laptop, y de tres años para un smartphone, en un periodo de 16 semanas (4 meses) los precio de las mismas serían 23,63 € para el primero y de 13,69 € para el segundo. Por otro lado, el tiempo de amortización del punto de recarga no se conoce todavía, pero con la creciente y rápida mejora de estas tecnologías se pueden asumir también unos 5 años, lo que hace un total de 65,56 €.

En el caso del ordenador al utilizarse un mayor número de recursos que en lo normal al utilizar un servidor web, bases de datos y servidores WebSocket se puede suponer una amortización estimada de 30 €. Por otro lado, el smartphone tiene una situación similar, por lo que se supone una amortización de 20 €. Sin embargo, el punto de recarga solo se ha utilizado para momentos puntuales, por lo que se considera que la amortización se mantiene en 65,56 €

5.4.1. Especificación de recursos

El ordenador se ha utilizado en todos los procesos realizados durante el trabajo.

- Se ha instalado el CSMS base (*Planet Charger* y los servidores websocket) sobre el que se han realizado los cambios.
- La base de datos del CSMS también se ha juntado en el mismo equipo. Para una buena práctica debería separarse en otra máquina, al igual que el CSMS.

Sin embargo, al tratarse de un sistema de pruebas no se ha considerado necesario.

- El proceso de desbloqueo del móvil para poder copiar las etiquetas RFID se ha realizado desde el mismo equipo.
- El punto de recarga estaba también conectado al equipo mediante un cable de red.
- La implementación de ambas soluciones, una mediante un editor de textos y la otra mediante *Android Studio* se han realizado en el mismo equipo.

Por otro lado el dispositivo móvil se ha utilizado para dos cosas.

- La copia de la etiqueta RFID y las pruebas de que se puede generar esta desde una app.
- El uso de la aplicación de 2FA para autorizar los inicios de recarga.

5.5. Gestión de riesgos

Todos estos procesos conllevan siempre asociado una posibilidad de que alguno de los equipos falle o se pueda perder algún tipo de información. Esto se trata en este apartado.

5.5.1. Identificación de riesgos

En los proyectos software hay cuatro tipos de riesgos:

- Riesgos técnicos: trata de riesgos relacionados con calidad, tecnologías utilizadas, requisitos, rendimiento, complejidad y fiabilidad.
- Riesgos externos: los que tratan de factores externos, como proveedores, legislación, clientes, mercado y condiciones climáticas o localización.
- Riesgos de la organización: los relacionados con financiación, recursos y dependencias entre las partes del proyecto
- Riesgos de la dirección de proyectos: relacionados con la gestión de las tareas, la estimación de la duración de las mismas y las dependencias entre sí.

Se han listado varios fallos relacionados con este proyecto como, por ejemplo:

- Un fallo en el ordenador que haría desaparecer todo lo realizado hasta ahora, además del CSMS y de la base de datos. Este es de tipo técnico.
- Cometer un error durante el proceso de desbloqueo y *root* del smartphone que dejaría inservible el dispositivo. Es también de tipo técnico.
- Puede haber problemas con la duración de las tareas si hay algún error en la asignación de tiempos. Es de tipo de dirección de proyectos.

5.5.2. Análisis de riesgos

Mediante el análisis de los riesgos identificados recogeremos datos sobre posibles retrasos, las respuestas a un riesgo y las formas de poder evitarlos:

- En el caso del ordenador un error en cualquier componente que no sea el disco duro sería salvable, dado que se pueden extraer con cierta facilidad los datos. Sin embargo, si el error está en el disco duro se perderá todo el trabajo. Por ello estos códigos referidos a las implementaciones se han ido subiendo a un repositorio de *GitHub*. En caso de algún error se perdería el tiempo utilizado desde la última copia de seguridad.

En el caso del dispositivo móvil incluso en algunos momentos del proceso de *root* se ofrece la opción de realizar copias de seguridad, algo que efectivamente se ha realizado. Se generaría en caso de algún error una pérdida económica al tener que reparar el dispositivo además del retraso temporal de tener que volver a desbloquearlo.

Los problemas en la gestión de duración de las tareas se pueden producir por problemas externos (suministro de clave de desbloqueo de smartphone por parte del fabricante) o internos (algún error en la programación que se haya visto tarde). El retraso sería el producido por la tardanza en resolver estos asuntos y una opción para poder evitarlo es el adelantar alguna otra tarea posterior en la medida de lo posible.

Capítulo 6

Solución

En este apartado se explicará, de forma clara, tanto el sistema del que se dispone como de las soluciones que se han implementado para mejorar los aspectos de seguridad tratados en este trabajo.

6.1. Descripción de la solución

Como se ha podido comprobar a lo largo de este trabajo, es relativamente sencillo el hecho de poder copiar la etiqueta de identificación de un dispositivo RFID para posteriormente poder replicarla, incluso con un smartphone con tecnología NFC implementada sin coste adicional.

Para poder reducir las posibilidades de ataque y complicar la posibilidad de reproducir este ataque, se han probado dos sistemas. El primero de ellos trata de un sistema de autenticación de doble factor (2FA), que es una forma de identificarse en el proceso con dos pasos en lugar de uno. Por ejemplo, en [2] se propone un sistema de autenticación MFA. En este trabajo el proceso será el siguiente:

6.2. El proceso de análisis y desarrollo

En primer lugar, se dispondría de una app para smartphone. Esta app actualizaría cada cierto tiempo una pantalla principal en la cual se verían durante otro tiempo los procesos de carga que esperan por el segundo paso de autenticación. En este trabajo la app se programa en el sistema operativo Android.

Para este segundo paso de autenticación podría haber varias opciones. Como se expresa en [13], podría ser una identificación por biometría. También existen las posibilidades de realizar un doble paso de tarjetas RFID como se propone en [5], en este caso tratándose de dos etiquetas adyacentes. Otra opción, que es la que se utiliza en este trabajo, se basaría en un código a recibir en el momento en el que se inicia el proceso de carga. Este código puede ser por SMS o por correo electrónico, eligiéndose el email en este caso porque no conllevaría un coste económico adicional.

Tras ello, se combinará este sistema con otro basado en una tarjeta basada en NFC variable, habiendo una comunicación previa entre la misma y el punto de recarga, registrando una semilla y jugando con la hora actual. Al no disponer de esa tecnología, se aprovechará la opción que nos proporciona la plataforma web que gestiona el CSMS de que un usuario pueda enviar una orden de inicio de recarga remota (RemoteStartTransaction), haciendo el CSMS todo el proceso de simulación de tarjeta NFC y de inicio de recarga.

Además, se tratará la configuración más segura para este punto de recarga, basándola en lo visto en el apartado anterior del protocolo OCPP. Esta configuración se realiza desde una plataforma disponible por parte del fabricante.

6.2.1. Método basado en 2FA

Este sistema cada vez es más habitual. Entre otros, es similar al utilizado en las aplicaciones bancarias, al de acceso a redes de empresas... En el caso de este trabajo funciona de la siguiente manera:

- En primer lugar al tratar de iniciar la recarga el usuario asociado al identificador de la tarjeta que se trata de autorizar recoge el email asociado a este en la base de datos sobre la que trabaja el CSMS envía un correo electrónico con un código de 6 dígitos asociado al intento de inicio de recarga.
- Posteriormente, en una app de Android programada para este trabajo y siempre que un usuario esté logueado se van realizando peticiones cada cierto tiempo. Estas peticiones consultan si hay alguna petición de inicio de recarga abierta por el propio usuario. En caso afirmativo, se verá en el listado de la pantalla principal de la app.
- Se pulsa sobre ella y se pide un código de seis dígitos para autorizarla. Tras introducirlo, se consulta si el código es correcto y, en caso afirmativo, se autoriza

la recarga con el identificador de etiqueta que se ha pasado por el cargador o que se ha enviado de manera remota.

Para este método, al enviarse un paquete Authorize además de preguntar al CSMS si el usuario que trata de iniciar la recarga tiene autorización para ello o no, se crea una entrada en una tabla de la base de datos del CSMS para que, al autorizar en la aplicación, se cree la petición RemoteStartTransaction.

6.2.2. Método basado en NFC con etiqueta aleatoria

Este sistema se ha probado de manera simulada. Es decir, se ha diseñado un sistema para hacerlo todo desde el CSMS. En los sistemas actuales para la recarga del coche eléctrico, como ya se trató anteriormente en el trabajo, hay la opción de enviar las peticiones de inicio de recarga desde una app o una web que interactúa con el CSMS. Igualmente, se podrían implementar en una tarjeta o sistema basado en NFC. Este sistema es similar al que se utiliza para la apertura y cierre a distancia de las puertas de los coches. Con todo ello, este método funciona de la siguiente manera:

- En primer lugar, para iniciar la recarga, se realizaría un intercambio previo de una semilla sobre la cual se va a descifrar el identificador de etiqueta del cliente. Para el funcionamiento de ello se necesitaría implementar algún método de doble paso de claves por la pantalla del punto de recarga. Por ello en este ejemplo la semilla ya estaría guardada en el sistema CSMS y sólo se haría el paso de tarjeta con la semilla mezclada con la hora.
- Este identificador de etiqueta se mezcla con la hora actual con el siguiente formato: YYYYMMDDhhmmss.
- Con ello, se envía el inicio de recarga. Al hacerlo de manera combinada con la autorización en doble factor, se realiza el proceso con la app de Android programada para este trabajo y, tras hacerse la comprobación de que, efectivamente, el usuario que recarga es el que se espera, ya se inicia correctamente el proceso de recarga.

Para este método no hay que hacer ningún cambio más en el sistema aparte de la simulación de esta tarjeta basada en NFC.

6.2.3. Diseño

Para implementar esto se requiere, en primer lugar, un sistema como el explicado en el capítulo 4. Tras ello, se añadirán las herramientas creadas para la mejora de la seguridad, las cuales no requieren en esta prueba un aumento de la estructura del sistema. En un caso real sí se añadiría una tarjeta NFC.

6.2.3.1. Diseño de sistema

En primer lugar, relacionado con lo se explicó , se utilizarán los siguientes elementos.

- Un ordenador que dará soporte tanto al CSMS como a la base de datos.
- Un punto de recarga.
- Un smartphone para iniciar recargas.
- Una tarjeta con una etiqueta RFID para las simulaciones previas y la prueba de concepto.
- Una manguera para simular una recarga.

Para esta simulación se conectarán tanto ordenador (CSMS y BD) como punto de recarga a la misma red y no siendo evidentemente necesario que los demás equipos estén conectados.

El CSMS utilizado se llama *Planet Charger*. Es un servidor web mediante el cuál, interactuando con la base de datos, se pueden realizar las siguientes acciones.

- Un resumen de los datos de recargas.
- Registrar y editar los cargadores conectados al CSMS y algunos de sus datos.
- Registrar y editar los usuarios con permiso para recargar y sus datos.
- Disponer de un histórico de recargas realizadas en los cargadores conectados al CSMS.
- Disponer de un histórico de los paquetes y peticiones intercambiadas entre cargadores y CSMS.
- Otros enlaces de interés como gráficas, tarifas...

En el caso de este trabajo lo interesante son tanto los cargadores conectados a los CSMS, los permisos de los usuarios y el registro de las recargas.

Este servidor web funciona con los lenguajes HTML, PHP, CSS y JavaScript.

- HyperText Markup Language (HTML) es el componente más básico de la Web, ya que define el significado y la estructura del contenido web. Se combina con otras tecnologías para describir la visualización de una página web (CSS) o comportamientos (JavaScript).
- Hypertext Preprocessor (PHP) es un lenguaje de código abierto adecuado para el desarrollo web y que puede ser incrustado en HTML. Se utiliza la versión 7.2.5.
- Cascading Style Sheets (CSS) es el lenguaje de estilos utilizado para describir la presentación de documentos HTML.
- JavaScript (JS) es un lenguaje de programación ligero, interpretado, o compilado justo-a-tiempo (just-in-time) conocido mayormente como un lenguaje de scripting (secuencias de comandos) para páginas web.

El servidor web que se utiliza es Internet Information Services (IIS). Este convierte a un ordenador en un servidor web tanto para Internet como para intranet, es decir, que en los equipos que tienen este servicio instalado se podrían publicar páginas web de forma local y de forma remota. Se basa en este caso en un módulo PHP. La versión que se utiliza en este trabajo es la 10.0.

La base de datos se basa en MariaDB. Este es un sistema de gestión de bases de datos derivado de MySQL con licencia GPL (General Public License). Se utiliza la versión 10.9.

Como se ha descrito anteriormente, la comunicación con el punto de recarga se realiza a través de WebSocket y utilizando el protocolo de comunicación OCPP 1.6.

Por otra parte, desde el propio ordenador y para facilitar el trabajo, se utiliza un gestor de puntos de recarga. Este puede ver los EVSE conectados a la misma red del ordenador en el que se ejecuta. La aplicación se llama *Ace Service Installer*.

Para las recargas se simulará una tarjeta NFC en lenguaje también PHP.

Se diseñará una app para sistemas operativos Android para completar la autenticación 2FA. Para ello se utiliza Android Studio y el lenguaje de programación Java.

6.2.3.2. Diseño detallado

En este apartado se describirán los aspectos más visuales del sistema y funcionamiento y, posteriormente, se tratarán las implementaciones realizadas para llevar cumplir los requisitos propuestos en el trabajo.

En primer lugar, el servicio web base utilizado, *Planet Charger*, dispone lógicamente en su inicio de una pantalla paraloguearse.



Figura 6.1: Pantalla de login de la web

Tras acceder a la plataforma, hay un menú lateral. En ese menú lateral los botones de *Datos*, *Usuarios*, *Plazas*, *Sesiones de recarga* y *Comunicación*.

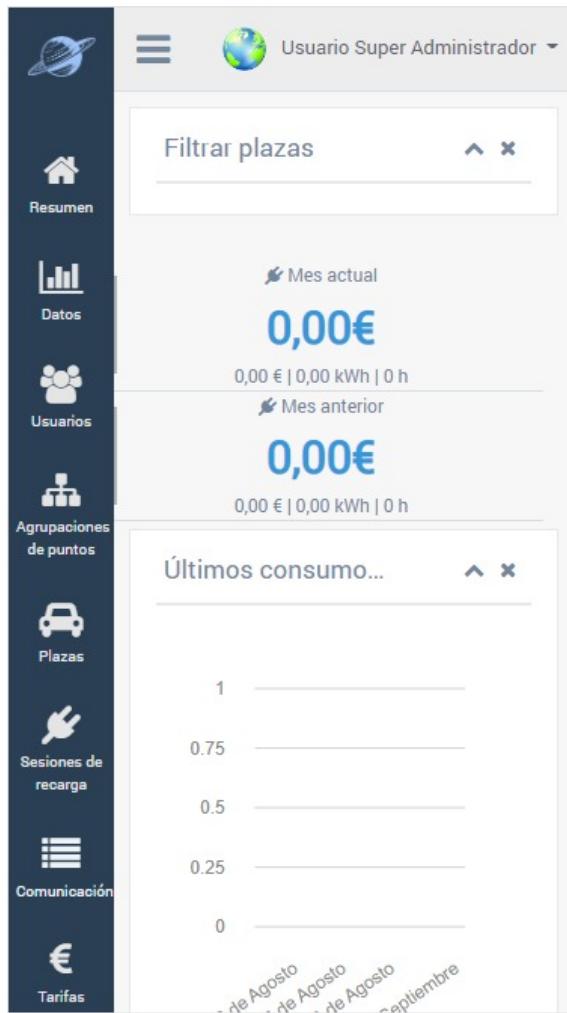


Figura 6.2: Pantalla principal de la web

Si se accede en el botón *Usuario* se dispone de un listado de los usuarios registrados en la aplicación. Al editar un usuario se ven varios datos. En el caso de este trabajo solamente nos interesan *e-mail* y *Semilla de UID de tarjeta*. El primero para la autenticación doble factor y el segundo para la tarjeta NFC, en este caso simulada.

The figure consists of two side-by-side screenshots of a web-based user management system. Both screenshots feature a top navigation bar with a globe icon and the text 'Usuario Super Administrador'.

Left Screenshot (User List):

- Header: 'Usuarios' and '+ Nuevo usuario'.
- Search: 'Filtrar' input field and search button.
- Table Headers: 'Nombre' and 'Apellidos'.
- Data Row: Miguel | López Soto | mlopes12@estudiantes.unileon.es.
- Table Headers: 'Usuario' and 'Rol'.
- Data Row: Super Administrador.
- Page Information: 'Mostrando 10 resultados' and 'Mostrando 1 a 2 de 2 resultados'.
- Pagination: 'Anterior 1 Siguiente'.

Right Screenshot (User Details):

- Header: 'Datos de usuario'.
- User Profile: Placeholder for a profile picture.
- Form Fields:
 - Nombre: Miguel
 - Apellidos: López Soto
 - e-mail: mlopes12@estudiantes.unileon.es
 - Semilla de UID de tarjeta: D2166181
 - Dirección: (empty)

Figura 6.3: Pantallas de usuario

Tras este, hay otros apartados de interés de la web. En *Plazas* hay dos enlaces, uno que lleva a un listado para editar los puntos de recarga y otro para comprobar su estado y dos botones, uno realizar algún tipo de operaciones sobre ellos, como reiniciarlos o realizar inicios y fines de recargas, y otro para consultar y cambiar la configuración general del EVSE.

The figure consists of two side-by-side screenshots of a web application interface. On the left, the title 'Gestión de plazas' is at the top, followed by a 'Filtrar' search bar, a dropdown for 'Mostrando 10 resultados', and a search input field. Below is a table with columns 'Nombre' and 'Agrupación', showing a single row for 'Plaza TFM' and 'TFM'. At the bottom, it says 'Mostrando 1 a 1 de 1 resultados' and has 'Anterior' and 'Siguiente' buttons. On the right, the title 'Estado de plazas' is at the top, followed by a 'Filtrar' search bar. Below is a table with columns 'MAC', 'Última actualización', 'Estado', and others. It shows one row for 'AlfenTFM' with '2022-09-01 12:03:24' in 'Última actualización', 'Libre' in 'Estado', and icons for settings and notifications. A 'Siguiente' button is at the bottom.

Figura 6.4: Pantallas referidas a puntos de recarga

Además del botón *Sesiones de recarga*, donde se encuentran las cargas realizadas, se dispone de otro botón llamado *Comunicación*. En el enlace *Eventos* se dispone de los paquetes enviados por el punto de recarga. Y en respuestas se ven las respuestas del sistema a estos paquetes enviados por el punto.

Cargador	Tipo	Contenido
Plaza TFM	BootNotification	
Plaza TFM	StatusNotification	Available#! oError
Plaza TFM	StatusNotification	Unavailable NoError
Plaza TFM	StatusNotification	Available#!

Ante	Agrupación	Cargador	Mensaje
1-09-28 22:02	TFM	Plaza TFM	[3,"Re Agent est","s","Ac d"]
1-09-28 27:28	TFM	Plaza TFM	[3,"Re Agent est","s","Ac d"]

Figura 6.5: Pantallas referidas a las comunicaciones con los puntos de recarga

Para la ejecución de la autenticación 2FA se ha implementado un pequeño módulo en el que se reciben las peticiones de inicio de proceso de recarga generadas para poder confirmarlas.

En este caso no se ha profundizado dado que se trata de un modelo simulado. Sin embargo, gran parte de las compañías que dan soporte a la recarga del vehículo del coche eléctrico disponen de aplicaciones, tanto en Android como en iOs, para realizar los procesos y controles que se hacen desde la app, al menos en la parte de llevar el control de procesos de recarga y de histórico de recargas del propio usuario. Por ello este módulo que se ha implementado como una entidad independiente podría integrarse sin problemas en una app de una compañía eléctrica.

En primer lugar, al igual que en el anterior sistema, se dispone de una pantalla de inicio de login en la que se deben introducir lógicamente los mismos datos que en la web.

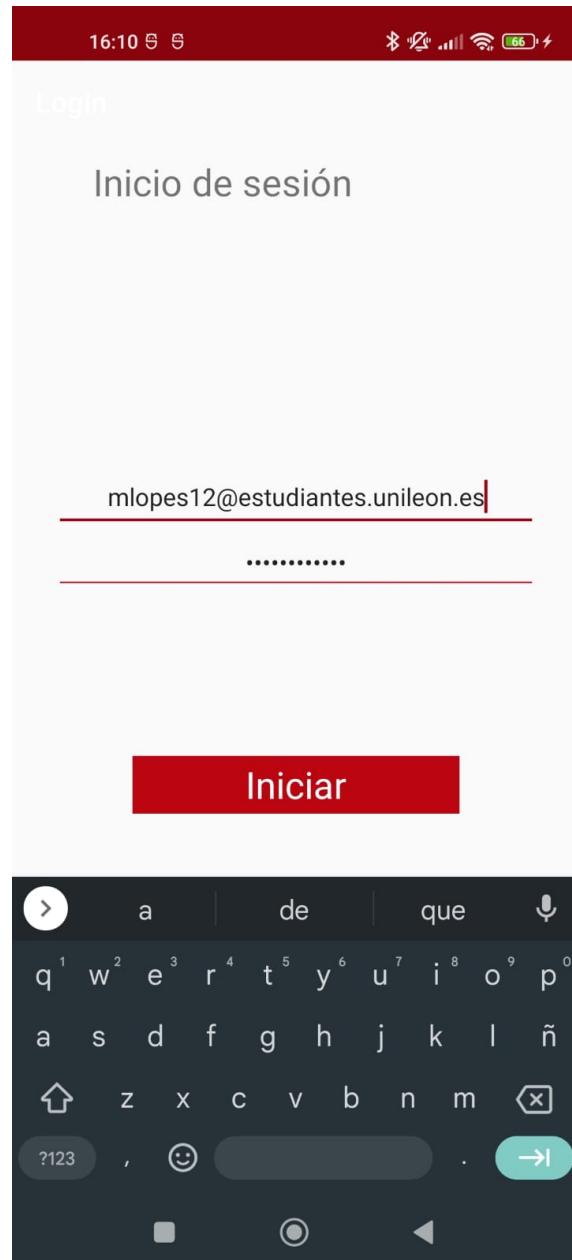


Figura 6.6: Pantalla principal de login de la app

Al acceder de forma correcta, se percibe el listado de recargas a finalizar su autenticación. Habitualmente sólo se verá una dado que lo habitual es un usuario cargando con un vehículo.

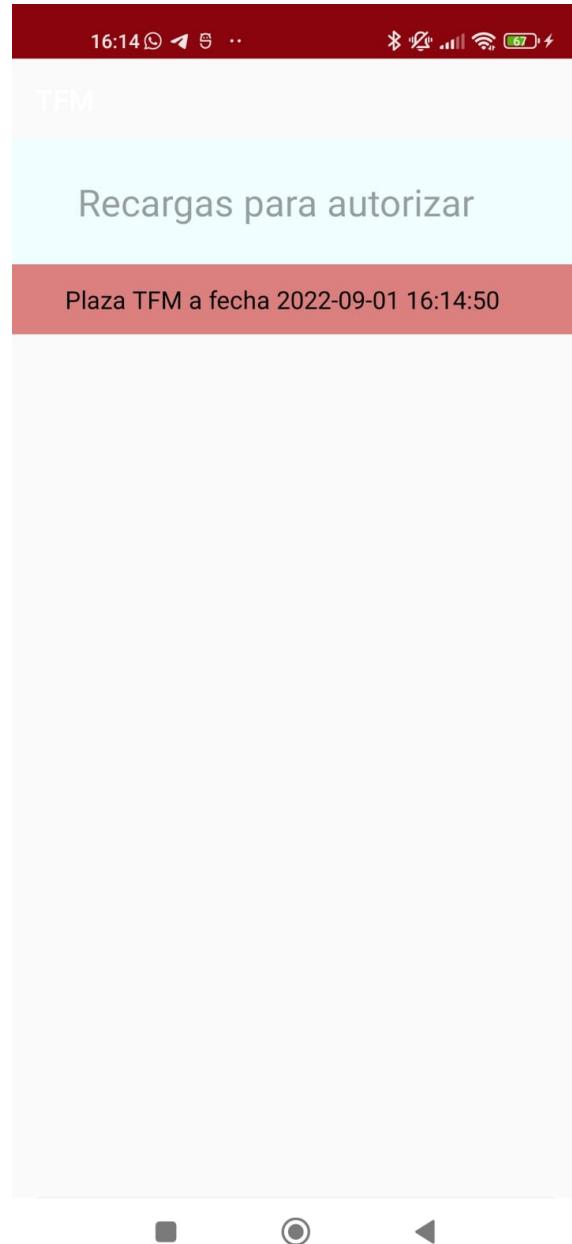


Figura 6.7: Pantalla con el listado de cargas a confirmar

Tras confirmarlo, se ve la pantalla en la que hay que insertar el código recibido por correo electrónico al iniciar el proceso de recarga.



Figura 6.8: Pantalla en la que introducir el código de confirmación de inicio de recarga

Como se ve, todo lo que hace este sistema, al igual que la app de Android es interactuar para añadir, editar y eliminar datos en la base de datos e iniciar o parar recargas.

6.2.4. Implementación

En este apartado se tratan los dos sistemas programados en este apartado, comparando los procesos actuales con los resultantes tras estos cambios. El código de los mismos se podrá encontrar en los anexos de este trabajo.

Para la realización de la autenticación 2FA se han realizado los siguientes pasos:

- Lo primero es la creación una tabla en particular en la base de datos con los campos:
 - *id_authorization* (identificador único de la solicitud de inicio de recarga)
 - *id_plaza* (identificador único de la plaza en la que se pretende iniciar recarga)
 - *idTag* (etiqueta de identificación con la que se pretende iniciar recarga)
 - *codigo* (código que se envía por email al usuario al que está asociado la tarjeta y que este tiene que introducir en la app para confirmar el inicio de recarga)
 - *fecha* (fecha de solicitud del inicio de recarga)
 - *validez* (tiempo en segundos de validez de la solicitud de inicio de recarga)
 - *id_individuo* (identificador único del individuo que pretende iniciar recarga)
 - *autorizada* (indica si se ha confirmado la solicitud de inicio o no)
 - *idTagCharge* (etiqueta de identificación con la que se inicia la recarga que es distinta a la de la tarjeta para evitar la posibilidad de que con la misma etiqueta que se inicia carga se pueda detener)
- Posteriormente, tanto en la función que interpreta los paquetes *Authorize* como en el *RemoteStopTransaction* añadir una función que introduzca una entrada en la tabla y que envíe un correo con un código PIN para realizar la autorización 2FA.
- La app, programada en Windows mediante *Android Studio*, realiza constantemente una consulta asíncrona a la base de datos con un identificador de usuario para ver cuáles son las recargas pendientes de la doble autorización.

- La app envía el código al servicio web, que comprueba si es correcto y contesta a la app. Si es correcto, se inicia la recarga. En caso contrario llegará un aviso de que es incorrecto.
- Para detener la recarga simplemente se debe realizar un paso de tarjeta o hacerlo desde la web.

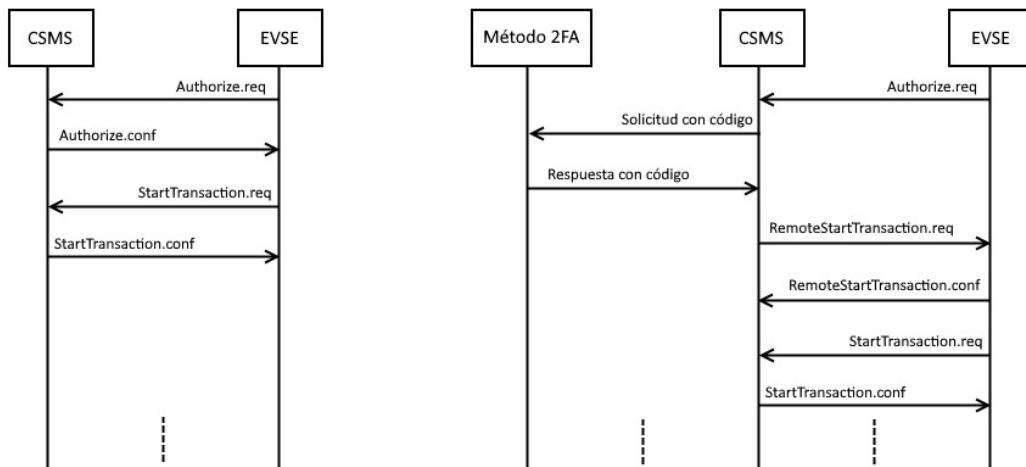


Figura 6.9: Diagrama de flujo del funcionamiento del protocolo OCPP 1.6 (izquierda) y añadiendo la autenticación 2FA (derecha) iniciando el proceso de recarga con una tarjeta

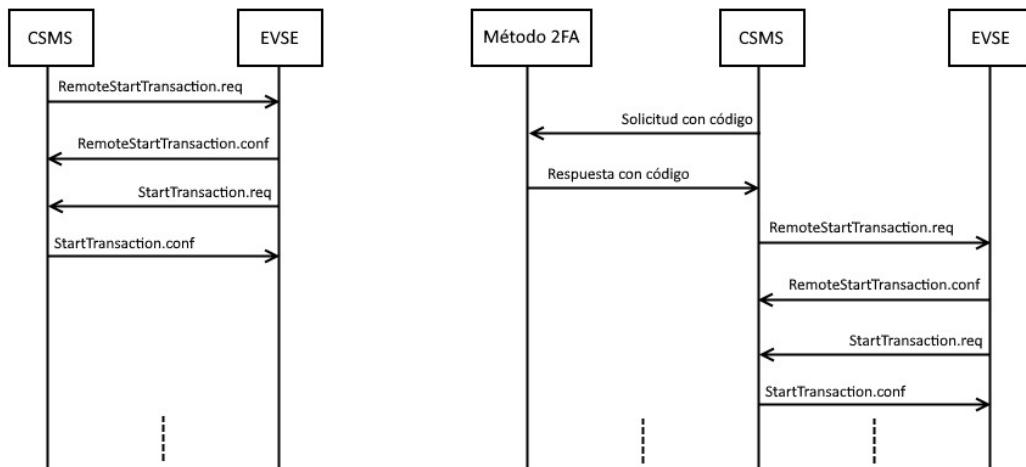


Figura 6.10: Diagrama de flujo del funcionamiento del protocolo OCPP 1.6 (izquierda) y añadiendo la autenticación 2FA (derecha) iniciando el proceso de recarga desde el CSMS

Para la simulación de la tarjeta NFC aleatoria:

- Se crea una función, la cual genera, a partir de una semilla, un número semi-aleatorio multiplicándola con la fecha y hora actuales en segundos.
 - La semilla hexadecimal sobre la que se va a calcular la etiqueta se pasa a decimal (para las simulaciones posteriores se recoge la etiqueta de una tarjeta RFID).
 - Se toma toda la fecha actual en segundos.
 - Los dos valores anteriores se multiplican y se convierten a hexadecimal.
 - Finalmente se recogen los catorce caracteres más significativos y, en caso de que haya menos de catorce, se añaden a la derecha tantos ceros como se necesiten hasta cubrir los catorce.
- En caso de que se detenga con la tarjeta se hace la misma generación a partir de la semilla en el *Authorize*, pero en este caso se añade la función a la comprobación. Al no poder pararse con una tarjeta distinta a la que inició recarga (eso sólo pasa cuando se produce una reserva antes de iniciar la recarga) se envía un *RemoteStopTransaction* siempre y cuando la tarjeta esté autorizada. En caso de que sea un *RemoteStopTransaction* desde la web no hay nada que modificar ya que no necesita de la etiqueta para detener la recarga.

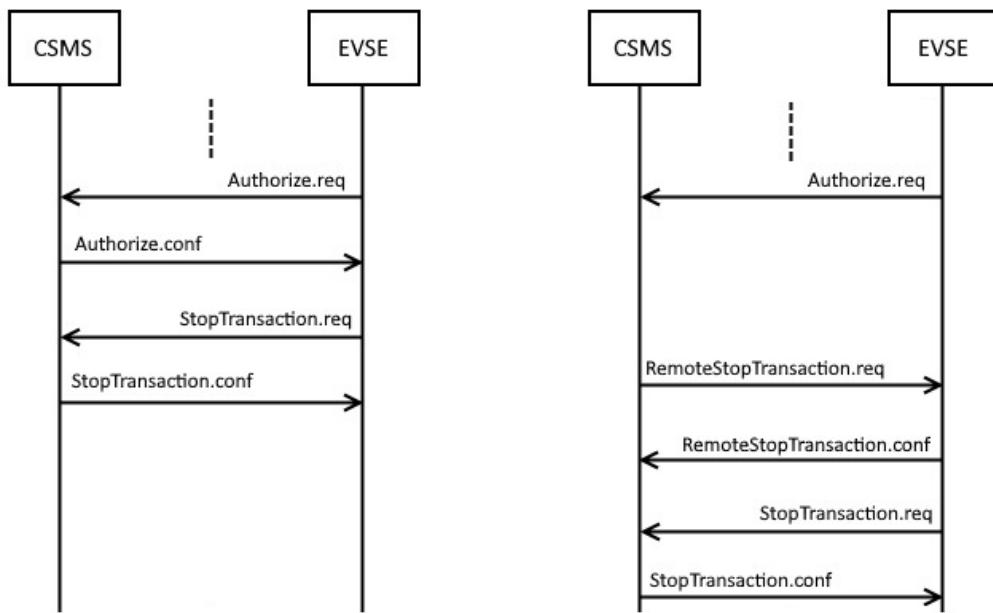


Figura 6.11: Diagrama de flujo del funcionamiento del protocolo OCPP 1.6 (izquierda) y añadiendo una etiqueta variable (derecha) finalizando el proceso de recarga con una tarjeta

Y, finalmente, el resultado definitivo se produce aplicando ambos criterios de forma simultánea. Dado que afectan a partes distintas del proceso no se modifican el uno al otro.

Sin embargo, para la simulación en los *Authorize* se hace una simulación modificando la etiqueta de una tarjeta no variable. Con ella se puede simular el comportamiento de una tarjeta NFC en los procesos que inicia el EVSE. Para los procesos que inicia el servicio web del CSMS esta simulación sería la implementación en código definitiva.

6.2.5. Pruebas

En este apartado se tratará, en primer lugar, la prueba de concepto, mediante la cual se prueba a realizar el ataque. Tras ello, se realizan pruebas de los instrumentos que ayudan a mejorar la seguridad de la autorización de recarga.

6.2.6. Prueba de concepto

La prueba de concepto o PoC (Proof of Concept) es la implementación de un método o de una idea que trata de verificar que el concepto o teoría en cuestión es susceptible de ser explotada de una forma realista.

En este apartado se describirá un posible caso real de robo del identificador de una tarjeta de fidelización de un cliente y los pasos seguidos para el mismo. Se dispone de un smartphone modelo Xiaomi Redmi Note 8T, mediante el cuál se procederá a leer una tarjeta con una etiqueta RFID. Desde ese mismo teléfono móvil se simulará la emisión del mismo código para que, con el propio móvil se pueda recargar como si fuese el usuario al cuál se le han robado los datos.

Es necesario conseguir *rootear* en primer lugar el dispositivo dado que es la única opción de simular la emisión de códigos de tarjetas distintos a los generados por el propio dispositivo. Este es el proceso que permite a los usuarios de dispositivos Android obtener algunos privilegios para modificar algunas funciones que vienen por defecto en estos dispositivos.

Para ello, en el caso de el dispositivo que se va a utilizar para esta prueba se deben activar, en primer lugar, las opciones de desarrollador. Se hace en la pantalla de ajustes, en el apartado *Mi dispositivo*, pulsando siete veces en *Versión de MIUI*.

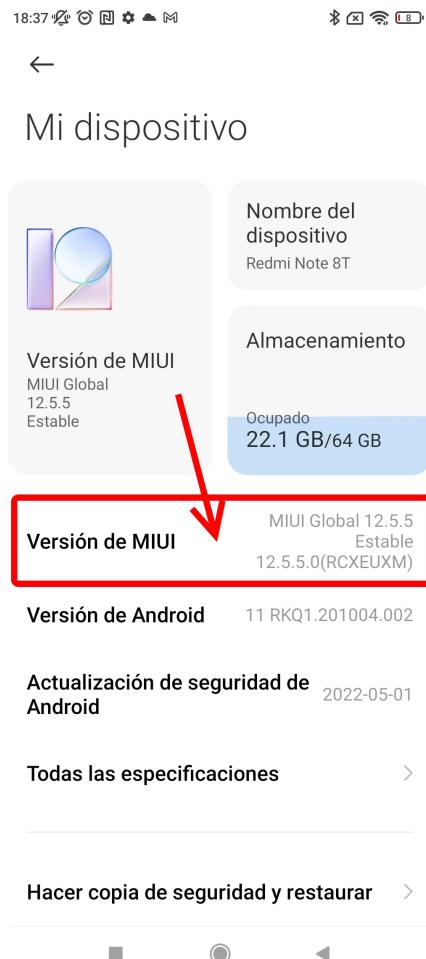


Figura 6.12: Pantalla de *Mi Dispositivo*

Posteriormente se debe desbloquear el *bootloader* (gestor de arranque) para poder instalar una *ROM* (versiones modificadas de Android) o rootear el dispositivo, y para ello se deben en primer lugar activar tanto la *depuración USB* como el *desbloqueo OEM*. Esto se hace nuevamente en los ajustes del dispositivo dentro de las opciones de *Ajustes adicionales* en los botones *Opciones de desarrollador* y *desbloqueo de OEM*. Se activan y dentro del desbloqueo OEM pedirá una cuenta de usuario del fabricante Xiaomi y disponer de una tarjeta SIM para continuar el proceso.

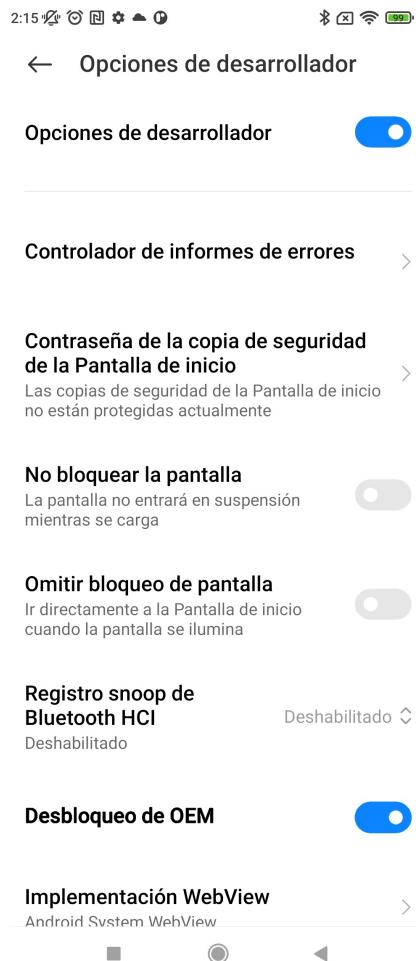


Figura 6.13: Pantalla de *Opciones de desarrollador*

Para realizar este desbloqueo se necesita disponer de un ordenador con sistema operativo Windows, dado que el programa que permite realizar este proceso (*Mi Unlock*) funciona en este tipo de sistemas, además de un cable USB para conectar el smartphone al mismo.

Se debe, por tanto, instalar ese programa e iniciar sesión en él con la cuenta de Xiaomi del propio dispositivo. Se apaga el teléfono y se enciende pulsando tanto el botón de encendido como el de volumen arriba para iniciararlo en un modo llamado *fastboot*. Se conecta al ordenador y se espera que el botón *Unlock* se sitúe en verde.

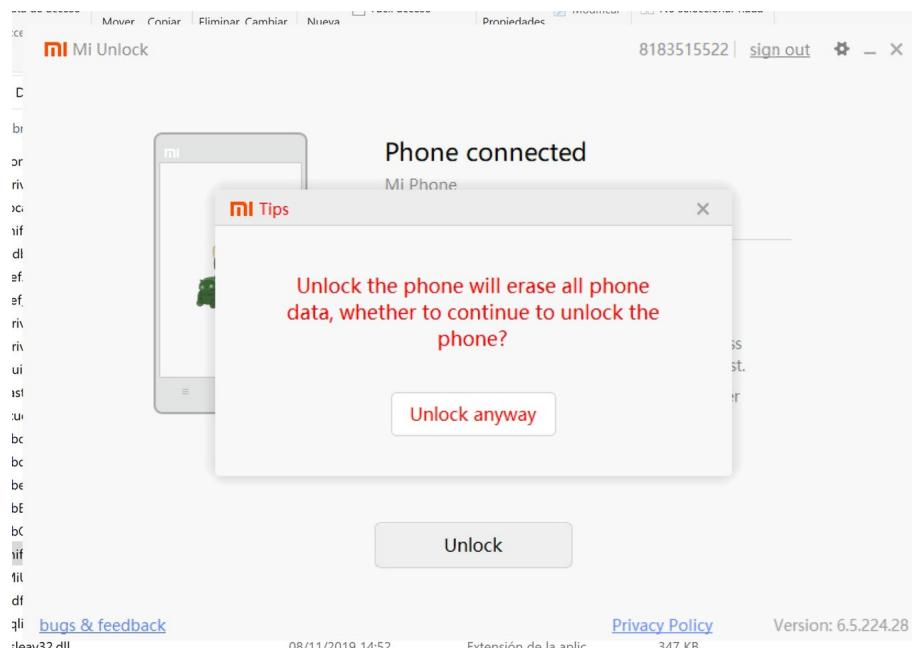


Figura 6.14: Pantalla de advertencia previa a desbloqueo de *Mi Unlock*

Tras aceptar, *Mi Unlock* comprueba que tanto cuenta como dispositivo son aptos. Si eso es así, el programa envía una solicitud a los servidores de Xiaomi con el dispositivo asociado. Tras ello, en la pantalla del programa aparecerá el tiempo que se debe esperar hasta el desbloqueo del dispositivo (siete días).

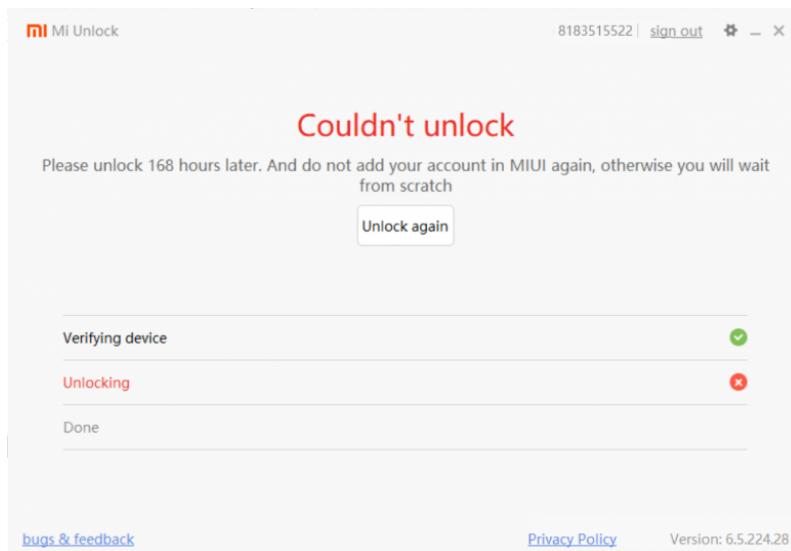


Figura 6.15: Pantalla de aviso de tiempo a esperar para desbloqueo de dispositivo mediante *Mi Unlock*

Tras transcurrir esa semana, se puede retomar el proceso de desbloqueo. Se repiten los mismos pasos con *Mi Unlock* y se espera a que finalice el proceso. En el caso de que

no se hubiera cumplido el tiempo de espera la aplicación informa de cuántas horas quedan para retomar este proceso. Antes de iniciar con el desbloqueo se deben hacer copias de seguridad dado que este proceso reestablece el dispositivo a los valores de fábrica.

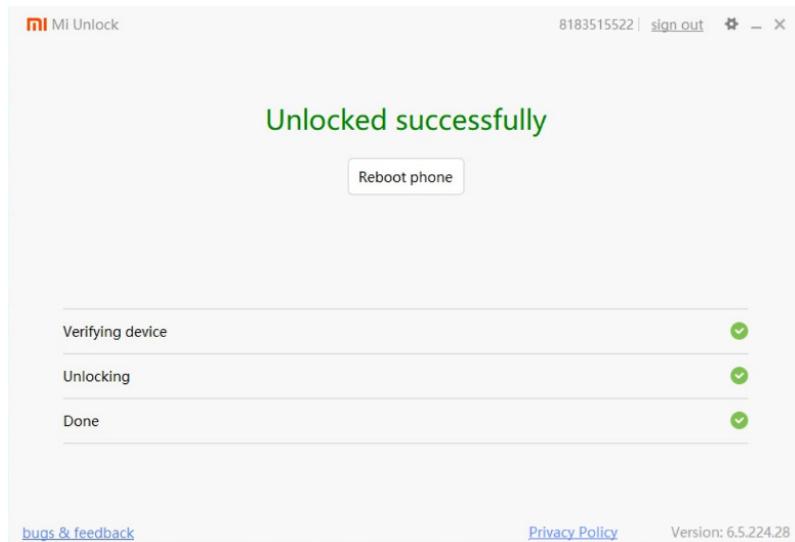


Figura 6.16: Pantalla de aviso de dispositivo correcto en *Mi Unlock*

Se debe volver a iniciar el dispositivo en modo *fastboot* para instalar el modo *recovery* (recuperador del sistema operativo) *TWRP* (*Team Win Recovery Project*, un recovery personalizado para instalar ROM, restaurar copias de seguridad, rootear el dispositivo...) para poder continuar con la prueba.

Además, hay que instalar el *Android Debug Bridge* (ADB), una herramienta de línea de comandos que permite realizar algunas acciones en el dispositivo, tales como instalar o depurar apps, y proporciona acceso a un shell para poder ejecutar distintos comandos en un smartphone.

Se vuelve a conectar el PC y se conecta el dispositivo a mediante un cable USB al PC con la depuración USB del mismo activada. En una ventana del símbolo del sistema, en la carpeta en la que se encuentran los drivers ADB se ejecuta el siguiente comando.

```
adb reboot bootloader
```

Con ello se inicia el dispositivo en modo *fastboot*.

Posteriormente, tras descargar la versión correspondiente de TWRP, se introducen los siguientes comandos desde el símbolo de sistema para actualizar al nuevo *recovery TWRP*.

```
fastboot flash recovery twrp.img
```

```
fastboot boot twrp.img
```

Tras ello, el nuevo modo *recovery* de este dispositivo será el de TWRP.

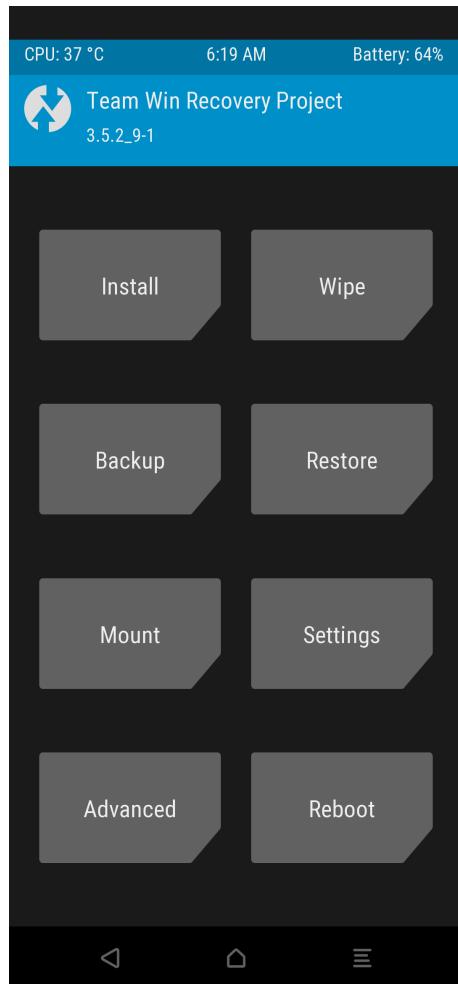


Figura 6.17: Pantalla principal de TWRP

Ya desde *TWRP* en primer lugar se formatea el equipo y se reinicia en modo *recovery* después para que quede correctamente instalado.

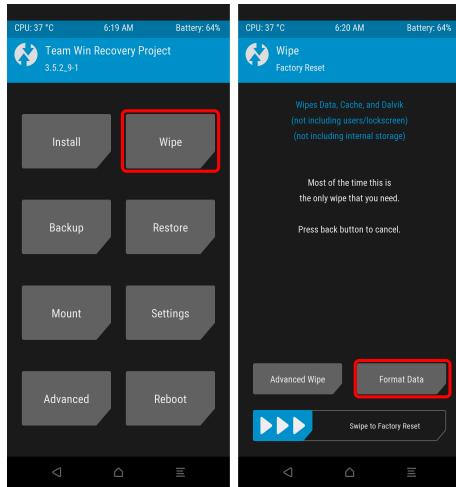


Figura 6.18: Proceso para formatear el dispositivo

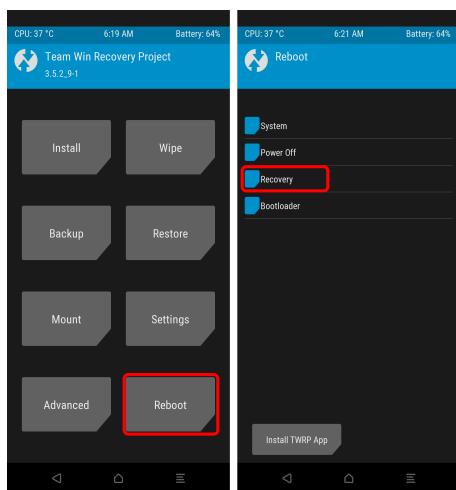


Figura 6.19: Proceso para reiniciar en modo recovery

En último lugar, se deben descargar y copiar al dispositivo las versiones correctas, según el dispositivo que se utilice, en extensión ZIP de los ficheros de instalación de Magisk y Disable_DM-Verity por ese orden para poder rootear el dispositivo.

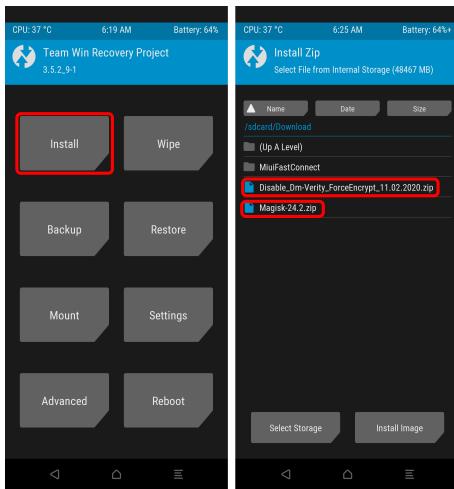


Figura 6.20: Proceso para instalar ficheros zip para rootear

Con todo ello, el smartphone quedará rooteado y ya se puede pasar a realizar la prueba.

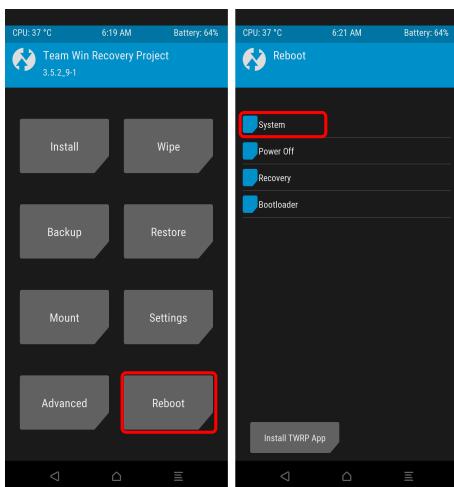


Figura 6.21: Proceso para iniciar el móvil en funcionamiento normal

Para ello, se instala la aplicación llamada *Emulador de tarjetas Pro (NFC Card Emulator Pro)*.

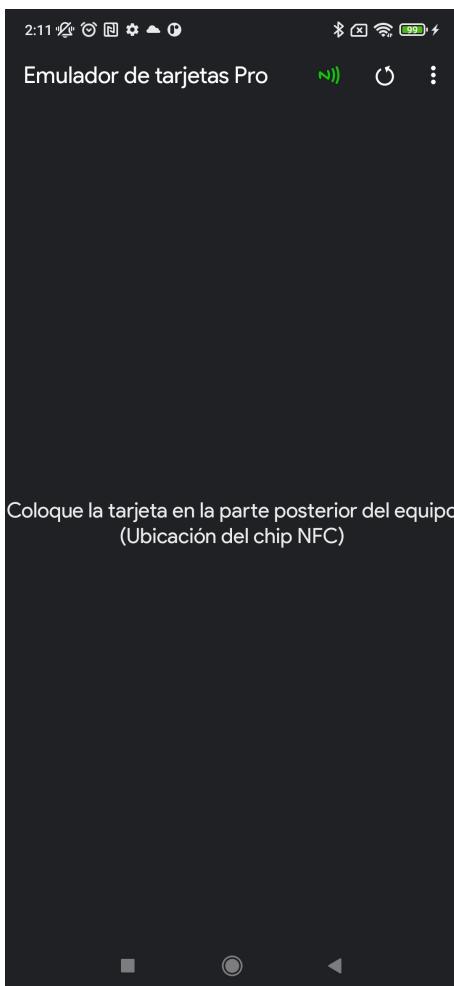


Figura 6.22: Pantalla de *Emulador de tarjetas Pro* tras instalar la app

Desde la app se indica que se coloque la tarjeta en la parte posterior del equipo para leerla tras pulsar al primer botón de la parte superior izquierda de la pantalla. Se lee la tarjeta para disponer de la etiqueta de la misma y se guarda en *Aceptar*.



Figura 6.23: Pantalla de *Emulador de tarjetas Pro* tras leer una tarjeta

Se pulsa en el ícono inferior derecho del interior de la tarjeta para emularla. Se acepta la solicitud de cualquier tipo de permiso. Con ello la tarjeta se emulará durante un tiempo en intervalos temporales cortos pero alternos, por lo que en varios momentos la tarjeta queda correctamente *copiada* para simular el número de etiqueta de la tarjeta.

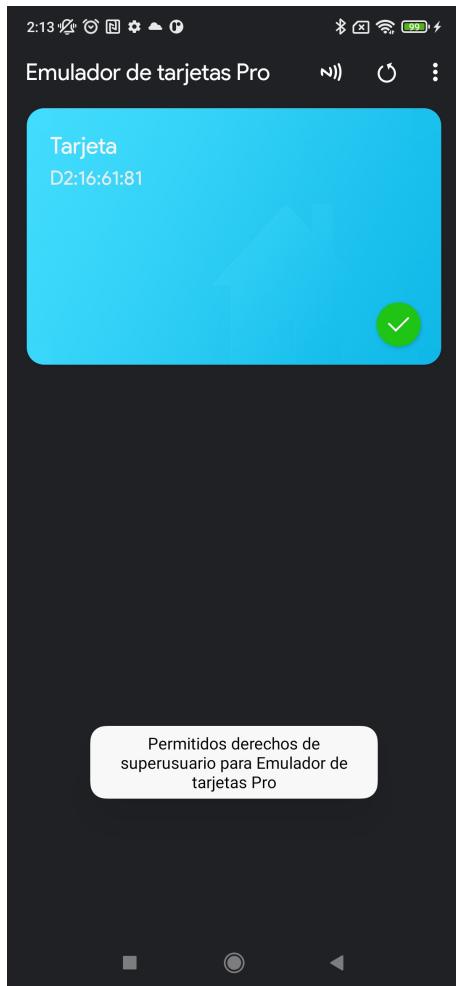


Figura 6.24: Pantalla de *Emulador de tarjetas Pro* durante la emulación de una tarjeta

Para comprobar que esto funciona correctamente, se realiza una prueba pasando la tarjeta sobre el cargador, el cuál envía al servidor Websocket un paquete de tipo *Authorize*. Las operaciones del cargador utilizado (*Alfen EVe mini*) se pueden revisar con el programa *Ace Service Installer* siempre y cuando este se encuentre en la misma red que el ordenador desde el que se accede a este programa.

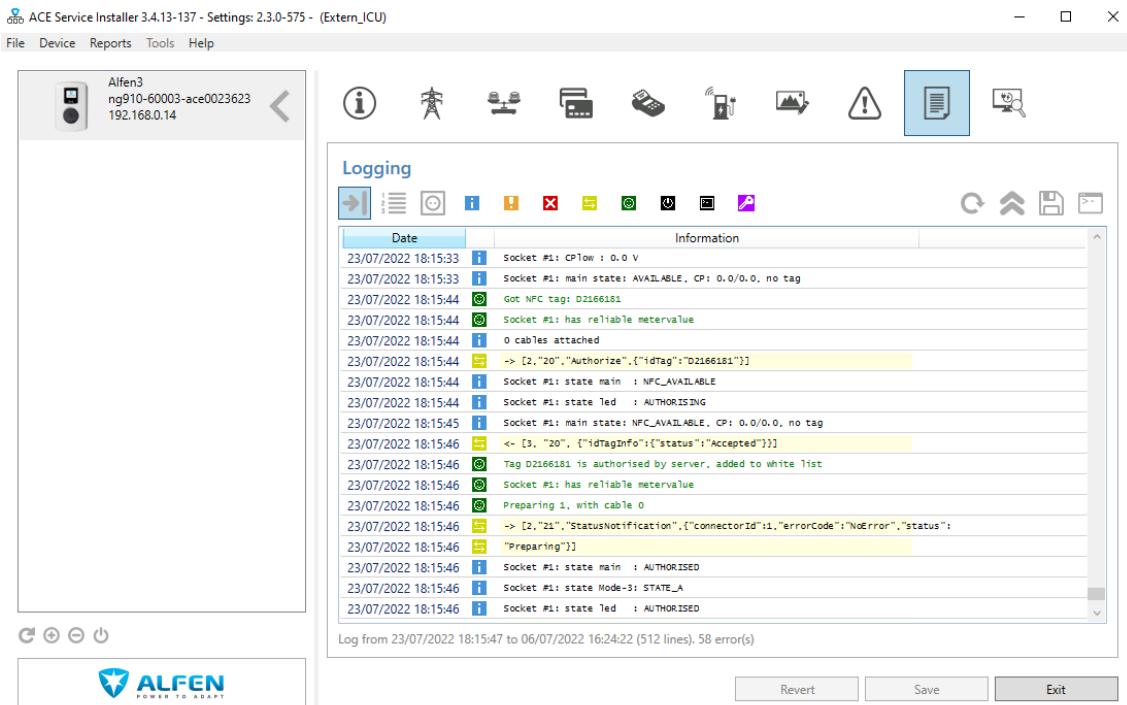


Figura 6.25: Pantalla de logs de Ace Service Installer tras el paso de tarjeta

Ahora, durante la emulación de la tarjeta, se pasa el smartphone por encima del punto de recarga para ver si el paso se produce correctamente. Se ve que, efectivamente, es así.

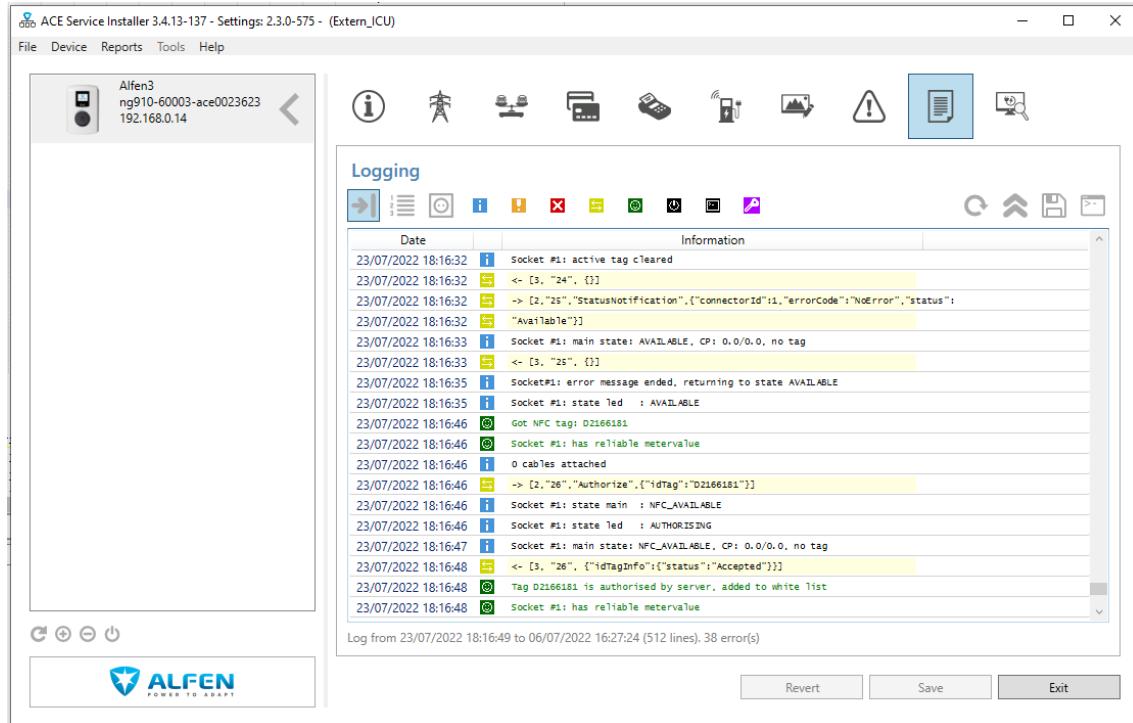


Figura 6.26: Pantalla de logs de *Ace Service Installer* tras el paso del smartphone que simula la tarjeta

Un caso similar a este se puede ver en el siguiente ejemplo de la página de *eventos de los cargadores* de la web.

The screenshot shows a web application interface for managing events. At the top, there is a navigation bar with a user icon labeled "Usuario Super Administrador". Below the header, the title "Eventos" is displayed. A "Filtrar" (Filter) section contains several dropdown and input fields:

- Tipo de eventos:** Authorize
- Agrupaciones:** TFM
- Plazas:** Plaza TFM
- Inicio:** 2022-07-23 (with time inputs 09 and 13)
- Fin:** 2022-07-24 (with time inputs 09 and 13)

Below the filter section is a blue "Filtrar" button. The main content area displays a table of event results:

Instante	Agrupación	Cargador	Tipo	Contenido	Más info.	Energía (kWh)	Usuario	Cardid	N.º carga
2022-07-24 08:53:58	TFM	Plaza TFM	Authorize			0	Usuario Tarjeta	D2166181	
2022-07-24 09:00:03	TFM	Plaza TFM	Authorize			0	Usuario Tarjeta	D2166181	
2022-07-24 09:06:23	TFM	Plaza TFM	Authorize			0		14B1EF62	
2022-07-24 09:06:27	TFM	Plaza TFM	Authorize			0		626CF731	
2022-07-24 09:06:31	TFM	Plaza TFM	Authorize			0		2623A34B	
2022-07-24 09:06:43	TFM	Plaza TFM	Authorize			0	Usuario Tarjeta	D2166181	

At the bottom of the table, it says "Mostrando 1 a 6 de 6 resultados". To the right, there are buttons for "Anterior" and "Siguiente".

Figura 6.27: Pantalla de eventos de la web tras los pasos de las etiquetas

6.2.7. Pruebas de posibles soluciones

6.2.7.1. Autenticación 2FA

En esta prueba se simularán un inicio tanto con un paso de tarjeta en el EVSE como una petición desde el servicio web.

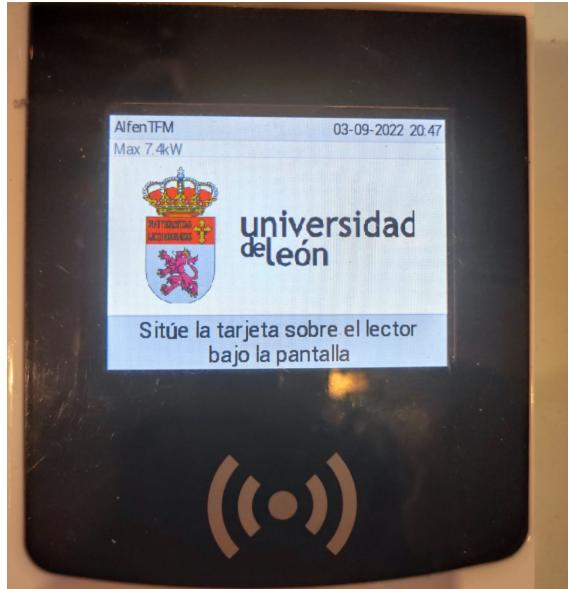


Figura 6.28: Pantalla del cargador en estado Libre

En el primero de los casos el cargador sí que cambia de estado, con una pantalla de espera.

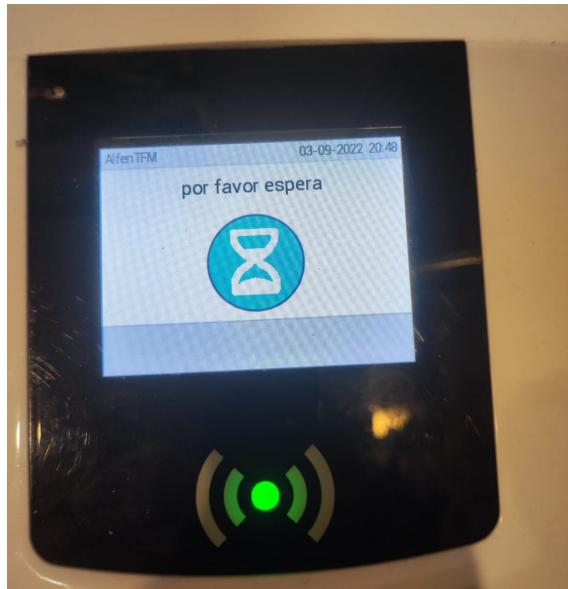


Figura 6.29: Pantalla del cargador tras enviar un Authorize

En el segundo, no hay ninguna modificación. A partir de aquí, el proceso es similar, llegando inmediatamente después de enviar la orden un correo electrónico con el código a introducir en la app.



Figura 6.30: Ejemplo de correo electrónico que llega al usuario al solicitar un inicio de recarga

Tras introducirlo, se envía una orden de recarga al cargador y este inicia la recarga.

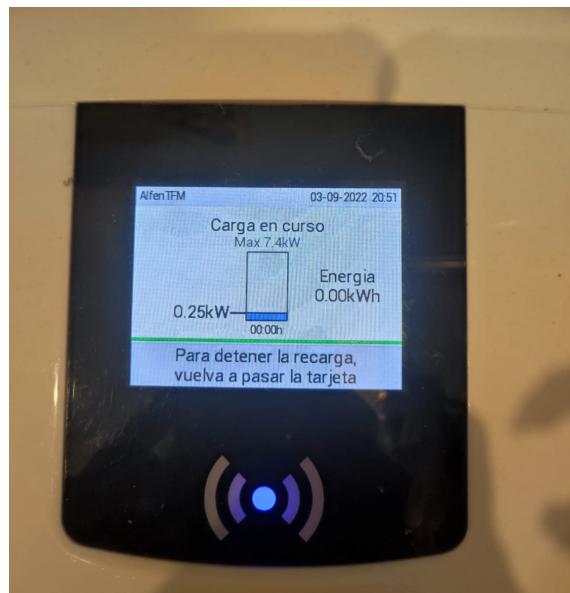


Figura 6.31: Pantalla del EVSE mientras se realiza una recarga

La comprobación más importante, que es el que el cargador vuelva a su estado original en caso de un paso de tarjeta si no se realiza la segunda autorización, funciona correctamente. En caso de que un usuario robase la etiqueta de tarjeta no dispondría de acceso al usuario en la plataforma de la persona que es la legítima propietaria de la misma.

6.2.7.2. Etiqueta NFC variable

En este caso lo interesante a probar es el paso de tarjeta mientras se realiza una recarga.

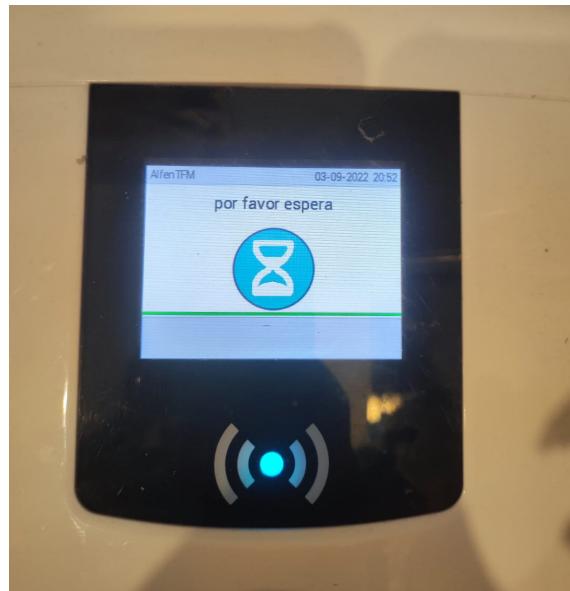


Figura 6.32: Pantalla del EVSE al pasar una tarjeta mientras se realiza una recarga

Si se pasa la misma tarjeta que inició la recarga esta no se debería detener dado que además de esta tarjeta variable se ha creado una *ficticia* en el inicio de recarga (se debe recordar que el propio cargador detiene una recarga iniciada con la misma etiqueta que se pase por el cargador al estar transcurriendo una recarga). Esto protege el sistema del robo de la etiqueta de la tarjeta al inicio de la sesión e impide que un usuario no autorizado pueda detener de algún modo la recarga del usuario que está cargando en ese momento.



Figura 6.33: Pantalla del EVSE al pasar una tarjeta mientras se realiza una recarga

6.2.7.3. Combinación de autenticación 2FA y etiqueta NFC variable

Como se dijo anteriormente, uno de los cambios afecta al inicio del proceso y el otro influye en la segunda parte. Por ello, combinándolas y realizando las mismas pruebas se obtiene

Capítulo 7

Evaluación

El objetivo de este trabajo era aumentar la seguridad en uno de los puntos del proceso de la recarga del coche eléctrico más vulnerables: la autorización del usuario. Al utilizarse un sistema con una simple etiqueta de identificación RFID, esta es sencilla de robar (como se vio en 6.2.6). Esto propicia el ataque de suplantación de identidad, en la que otro usuario se haría pasar por el usuario autorizado para recargar sin su consentimiento.

Para ello se han propuesto las dos soluciones tratadas. La primera, autenticación 2FA, está referida al software, por lo que se podría añadir con los sistemas actuales, dado que solo añadiría un punto intermedio en el proceso de inicio de recarga. Para la segunda se necesitaría una mayor infraestructura para comprender las tarjetas variables, que estas de algún modo dispusieran de un temporizador o algún tipo de contador para reproducir el sistema y que el punto de recarga fuese capaz de comprender de algún modo esta información.

7.1. Proceso de evaluación

7.1.1. Forma de evaluación

En ambos casos se han tratado de realizar varias suplantaciones de identidad, utilizando la etiqueta de la tarjeta con permiso en ambas. Con el funcionamiento actual del protocolo OCPP en ambos casos debería producirse esta suplantación, iniciando y deteniendo recarga.

Para poder determinar si la solución es correcta se debe hacer el mismo proceso de robo de tarjeta y ver que en uno de los casos no inicia la recarga y en el otro no se detiene. Viendo esto y no observando ninguna pérdida de funcionalidad se deberían dar por buenas ambas soluciones.

7.1.2. Casos de prueba

7.1.2.1. Autenticación 2FA

Al añadir ese punto intermedio del código de confirmación, por mucho que se disponga de los datos de etiqueta del usuario autorizado si no se dispone de los datos de acceso a la plataforma de la persona autorizada no se podrá iniciar la recarga.

7.1.2.2. NFC variable

En este caso hay que tratar de evitar que, aún robando el usuario la etiqueta con la que se inicia la recarga, esta no se pueda detener. Por ello, en primer lugar, aunque se pase una tarjeta, la etiqueta asociada a la recarga tiene que ser un número aleatorio. Esto es debido a que el cargador de forma independiente puede terminar la recarga con la etiqueta con la que la inició.

Podría no ser necesario el uso de una tarjeta variable. Sin embargo, si no se introduce, en el momento de comprobar los permisos en el CSMS también la detendría (no dependería de una semilla y un contador, fecha...).

Por ello, las pruebas realizadas fueron tratar de detener la recarga con la misma etiqueta con la que se inició, observando que al utilizarse una tercera etiqueta variable la recarga no se detiene. Si faltasen o la etiqueta aleatoria asociada a la recarga o la tarjeta NFC semialeatoria se podría utilizar perfectamente la misma etiqueta.

7.2. Análisis de resultados

Con todo ello, los resultados obtenidos pueden ser considerados como satisfactorios dado que, con estas dos nuevas características, sería necesario algo más que robar la etiqueta con permiso para poder cometer una suplantación de identidad:

- En el primero de los casos (2FA) el usuario atacante debería conocer el código de la autorización a la que se asociará la recarga y los datos de acceso a la plataforma del usuario con permisos para poder introducir el mismo.
- En el segundo de ellos (NFC variable) habría que conocer la semilla y los cálculos y procedimientos que se realizan para calcular las posibles etiquetas que se generarían a partir de ellas.

Todo ello aporta mucha más seguridad a esta parte del proceso de recarga.

Conclusiones

La evolución de la ciberseguridad de este tipo de sistemas es constante y muy elevada, sin embargo todavía se ven muchos aspectos mejorables. En tecnologías como RFID y NFC la seguridad ya está en un punto bastante avanzado a pesar de que, como se puede ver en el estado el arte, esta es muy mejorable y lógicamente está en constante mejora.

Por otra parte, en los sistemas de recarga del coche eléctrico todavía se necesita realizar un gran desarrollo en la seguridad. Sobre todo es necesario porque se trata de un campo que está utilizándose y extendiéndose prácticamente con un crecimiento exponencial por lo que las amenazas son cada vez mayores. Además, como se puede ver en este trabajo algunas de las vulnerabilidades son fácilmente explotables, como la suplantación de identidad vista. Al tratarse de una tecnología en la que entra en juego también sistemas de gestión, bases de datos, páginas web..., las amenazas se multiplican por cada utilidad añadida a este tipo de redes. El protocolo visto, OCPP, comienza en sus versiones más recientes a darle más importancia a la seguridad, añadiendo un mayor control a este tipo de sistemas.

Aportaciones realizadas

Este trabajo cuenta con varios puntos clave.

- En primer lugar se ha hecho una revisión de todos los trabajos realizados hasta la fecha en torno a la seguridad de las comunicaciones basadas en RFID y NFC, y por otro lado a la situación actual, tanto de seguridad como de situación de las tecnologías, del proceso de recarga del coche eléctrico.

Tras ello y centrándolo en la vulnerabilidad más fácil de explotar (suplantación de identidad robando la tarjeta) se han aportado dos diseños

- Referido a una modificación de software del CSMS, se ha añadido una autenticación de doble factor (2FA) basada en un generador de peticiones de inicio de recarga asociadas a códigos y un formulario para introducir estos códigos y autorizar estos inicios de recarga.
- En torno a una modificación del software del CSMS, y simulando una modificación de hardware, que sería externa al punto de recarga (una tarjeta NFC con una etiqueta variable con un contador, la fecha actual...) poder autorizar los inicios y los fines de recarga con una etiqueta distinta. Esto emula de algún modo los sistemas de seguridad de apertura mediante control remoto de vehículos en la propia automoción.

Trabajos futuros

En el planteamiento general inicial del trabajo se propusieron además dos casos posibles de estudio.

- Un lector biométrico para poder autorizar al usuario desde el punto de recarga. Para lo que se busca en este proyecto, que es no realizar modificaciones de hardware o software sobre el punto de recarga, sería imposible de realizar. Sin embargo, es una línea interesante a tratar por parte de los fabricantes de cargadores destinados al coche eléctrico.
- Una idea más sería la de añadir un teclado o una pantalla táctil para introducir un código de usuario para autorizar la recarga. Sería un doble factor (2FA) igual que el que se ha diseñado en este proyecto pero, al igual que en el caso anterior, requeriría la modificación del hardware del punto de recarga.
- Se estudiaron otras posibilidades que no afectasen al hardware pero que, seguramente, no solucionarían totalmente el problema actual del robo de tarjetas. Por ejemplo, el uso de una secuencia de dos etiquetas. Esto es más cómodo para el usuario pero se podría realizar igual el robo de etiquetas aunque este sería más complicado al necesitarse el robo de las dos.
- Otras opciones pero, en este caso, también tratando el hardware del vehículo, sería la opción de una comunicación del vehículo con el punto a través de la manguera o a distancia con un código RFID o NFC.

Además de ello, sería interesante mejorar los procesos aportados con las nuevas tecnologías que vayan lanzándose al mercado para poder mejorar la experiencia del usuario.

Problemas encontrados

A pesar de que el protocolo OCPP tiene unas pautas bastante claras, fuera de ellas puede haber algún cambio según el fabricante, por lo que sería interesante probar este sistema en un mayor número de marcas de EVSE. Un ejemplo de ello es el poder detener las recargas con el mismo identificador con el que se inició. Sería una opción a tener en cuenta que en versiones más modernas del protocolo esto se solucione, dado que reduce trabajo para mejorar la seguridad y mejora la experiencia también del cliente.

Otro problema encontrado en la prueba de concepto es que, a pesar de que el proceso de desbloqueo y *root* del smartphone es muy sencillo, el tener que esperar una semana al fabricante utilizado provocó tener que alterar, no tanto en tiempo como en redistribuirlo hacia la redacción de esta memoria. Probablemente en otros fabricantes de dispositivos móviles esto no suceda. Y en la misma línea en ocasiones los programas de emulación de tarjeta generan algún tipo de problemas.

Opiniones personales

En este trabajo se aporta una solución basada en una autenticación 2FA que puede dar problemas en lugares donde la cobertura es baja (párkings), lo que puede empeorar la experiencia del cliente. Respecto a la otra solución que se propone, probablemente las simulaciones de tarjetas NFC que se proponen en este trabajo sean más costosas y, en caso de realizarse todos los procesos mediante la app también se podrían dar problemas de cobertura.

En resumen, estas tecnologías, y más en la actualidad, están en constante crecimiento. El paso de la automoción basada en combustibles fósiles a electricidad es algo que se está acelerando y, al tratarse de sistemas conectados entre sí (IoT) es más fácil que surjan las vulnerabilidades y cuanto mayor número de personas los utilicen, mayor número de posibles vulnerabilidades. Además, estos sistemas actualmente disponen de muchas limitaciones a la hora de añadir algún tipo de comprobación extra de seguridad. Además de en los protocolos de comunicaciones, los fabricantes debe-

rían añadir componentes hardware y software que mejorasen la seguridad. Se está corriendo un cierto riesgo al lanzar estos productos quizá sin las mejores medidas de ciberseguridad.

Lista de referencias

- [1] W. Cao, S. Geng, X. Peng, J. Nie, X. Li y P. Li, "A Lightweight Encryption Algorithm for RFID System," 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), págs- 1094-1097, 2022.
- [2] M. S. Chishti, C. T. King y A. Banerjee, "Exploring Half-Duplex Communication of NFC Read/Write Mode for Secure Multi-Factor Authentication," en IEEE Access, vol. 9, págs. 6344-6357, 2021.
- [3] U. Ali et al., "RFID Authentication Scheme Based on Hyperelliptic Curve Signcryption," en IEEE Access, vol. 9, págs. 49942-49959, 2021.
- [4] Y. Yilmaz, V. -H. Do y B. Halak, "ARMOR: An Anti-Counterfeit Security Mechanism for Low Cost Radio Frequency Identification Systems," en IEEE Transactions on Emerging Topics in Computing, vol. 9, número 4, págs. 2125-2138, 1 de octubre-diciembre 2021.
- [5] H. Xu, X. Yin, F. Zhu y P. Li, "An Enhanced Secure Authentication Scheme With One More Tag for RFID Systems," en IEEE Sensors Journal, vol. 21, número 15, págs. 17189-17199, 1 de agosto de 2021.
- [6] C. Palli, N. Jampala y T. A. Naidu, "Sponge based lightweight authentication mechanism for RFID tags," 2021 4th International Conference on Security and Privacy (ISEA-ISAP), págs. 1-7, 2021.
- [7] Z. Leyu, Z. Xinyou, F. Yunjia, L. Shuyao, B. Jun y H. Xijia, "Design and Implementation of RFID Access Control System Based on Multiple Biometric Features," 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), págs. 570-575, 2021.
- [8] Y. Luo, K. Fan, X. Wang, H. Li y Y. Yang, "RUAP: Random rearrangement block matrix-based ultra-lightweight RFID authentication protocol for end-edge-cloud

- collaborative environment," en *China Communications*, vol. 19, número 7, págs. 197-213, julio de 2022.
- [9] Z. Pourmirza y S. Walker, "Electric Vehicle Charging Station: Cyber Security Challenges and Perspective," 2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE), págs. 111-116, 2021.
- [10] Z. Garofalaki, D. Kosmanos, S. Moschoyiannis, D. Kallergis y C. Douligeris, "Electric Vehicle Charging: A Survey on the Security Issues and Challenges of the Open Charge Point Protocol (OCPP)," en *IEEE Communications Surveys & Tutorials*, vol. 24, número 3, págs. 1504-1533, ultimo cuatrimestre de 2022.
- [11] H. Van Den Brink y P. Broos, ""Cyber security challenges in the electric vehicle infrastructure," CIRED Porto Workshop 2022: E-mobility and power distribution systems, págs. 429-432, 2022.
- [12] P. R. Babu, A. G. Reddy, B. Palaniswamy y A. K. Das, "EV-PUF: Lightweight Security Protocol for Dynamic Charging System of Electric Vehicles Using Physical Unclonable Functions," en *IEEE Transactions on Network Science and Engineering*, 2022.
- [13] M. Hataba, A. Sherif, M. Elsersy, M. Nabil, M. Mahmoud y K. H. Almotairi, "Privacy-Preserving Biometric-based Authentication Scheme for Electric Vehicles Charging System," 2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), págs. 86-91, 2021.
- [14] P. R. Babu, R. Amin, A. G. Reddy, A. K. Das, W. Susilo y Y. Park, "Robust Authentication Protocol for Dynamic Charging System of Electric Vehicles," en *IEEE Transactions on Vehicular Technology*, vol. 70, número 11, págs. 11338-11351, noviembre de 2021
- [15] P. V. Nikitin, K. V. S. Rao y S. Lazar, "An overview of near field UHF RFID", *IEEE RFID. Conferencia*, págs. 167-174, 2007.
- [16] M. M. Singh, K. A. A. K. Adzman, y R. Hassan, "Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures", *International Journal of Engineering & Technology Vol.7, N°4.31*, págs. 298-305, 2018.
- [17] ISO/IEC 18092. "Near Field Communication: interface and protocolo", 2004.
- [18] ECMA International (2005). "Near Field Communication - White Paper", Ecma/TC32-TG19/2005/012, 2005.
- [19] "NFC Data Exchange Format (NDEF), NFC Forum Technical Specification"

- [20] “NFC-Near Field Communication, Reader/Writer Operating Mode”
- [21] Fahrifianto F., Lubis M. F. y Fiade A., “Denial-of-service attack possibilities on NFC technology”, 2016 4th International Conference on Cyber and IT Service Management, IEEE, págs.1-5, 2016
- [22] Eun H., Lee H. y Oh H., “Conditional privacy preserving security protocol for NFC applications”, IEEE T. Cons. Electr., Vol.59, N°.1, págs.153-160, 2013
- [23] Kitchenham, B.A., Budgen, D., Brereton, P. “Evidence-Based Software Engineering and Systematic Reviews”, vol. 4. CRC Press (2016)
- [24] Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., ATP Group. “Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement”. Ann. Internal Med. 151(4) (264–269), 2009.
- [25] Saalfeld, C. “E-Mobility–Vehicle2Grid Interface. Vector-Kongress”, 2010
- [26] Bedogni, L., Bononi, L., Di Felice, M.; D’Elia, A.; Cinotti, T.S., “A Route Planner Service with Recharging Reservation: Electric Itinerary with a Click”. IEEE Intell. Transp. Syst. Mag. (8, 75–84), 2016.
- [27] Bedogni, L., Bononi, L., D’Elia, A., Di Felice, M., Rondelli, S., Cinotti, T.S. “A Mobile Application to Assist Electric Vehicles’ Drivers with Charging Services” (78–83). En las actas de la Eighth International Conference on Next Generation Mobile Apps, Services and Technologies, Oxford, UK, 10 al 12 de septiembre de 2014.
- [28] Rhode, K. “Electric Vehicle Cyber Research SANS Automotive Cybersecurity Workshop”, 2017
- [29] Shezaf, O., “Who can hack a plug? The Infosec Risks of Charging Electric Cars”, 2013.
- [30] Fearn, F. Kaspersky, V3 news, “Warning over electric car charging”, Enero de 2018.
- [31] Kocher, Paul, et al. “Security as a new dimension in embedded system design.” Actas de la 41.^a Conferencia anual de Automatización del Diseño. ACM, 2004.
- [32] Khelladi, Lyes, et al. “On security issues in embedded systems: challenges and solutions.” International Journal of Information and Computer Security 2.2, 2008.

- [33] Buamod I., Abdelmoghith E., Mouftah H.T., “A review of OSI-based charging standards and eMobility open protocols”. En actas de la 2015 International Conference on the Network of the Future, NOF 2015, Montreal, QC, Canada, del 30 de septiembre al 2 de octubre del 2015.
- [34] Schmutzler J., Andersen C.A., Wietfeld C., “Evaluation of OCPP and IEC 61850 for smart charging electric vehicles”. World Electr. Veh. J., 2013
- [35] Home - Open Charge Alliance. Web: <https://www.openchargealliance.org/>.
- [36] Wan, Kaiyu, K. L. Man, y D. Hughes. “Specification, Analyzing Challenges and Approaches for Cyber-Physical Systems (CPS).” Engineering Letters 18.3, 2010.
- [37] Orojloo, Hamed, y Mohammad Abdollahi Azgomi. “A method for modeling and evaluation of the security of cyber-physical systems.” Information Security and Cryptology (ISCISC), 11^a Conferencia Internacional ISC sobre IEEE, 2014.

Anexo A

Control de versiones

Para gestionar el código creado se ha utilizado GitHub como servicio de control de versiones. Se crea una cuenta con el usuario de correo de la Universidad de León y, con ello, se ha creado un repositorio. En él se encuentran:

- Carpeta de proyecto de aplicación de Android: <https://github.com/mlopes12/TFM/tree/main/App>
- Carpeta con el código y su explicación en un fichero *readme*: <https://github.com/mlopes12/TFM/tree/main/Web>
- Carpeta con la memoria: <https://github.com/mlopes12/TFM/tree/main/TFM>
- Carpeta con otro material (vídeos): <https://github.com/mlopes12/TFM/tree/main/Otros>

Anexo B

Seguimiento de proyecto fin de máster

B.1. Forma de seguimiento

Se han realizado reuniones semanales desde abril.

Estas se han realizado de manera telemática mediante la utilización de la utilidad GoogleMeet, ofrecida en este caso para las cuentas de usuario de la Universidad de León.

B.2. Planificación inicial

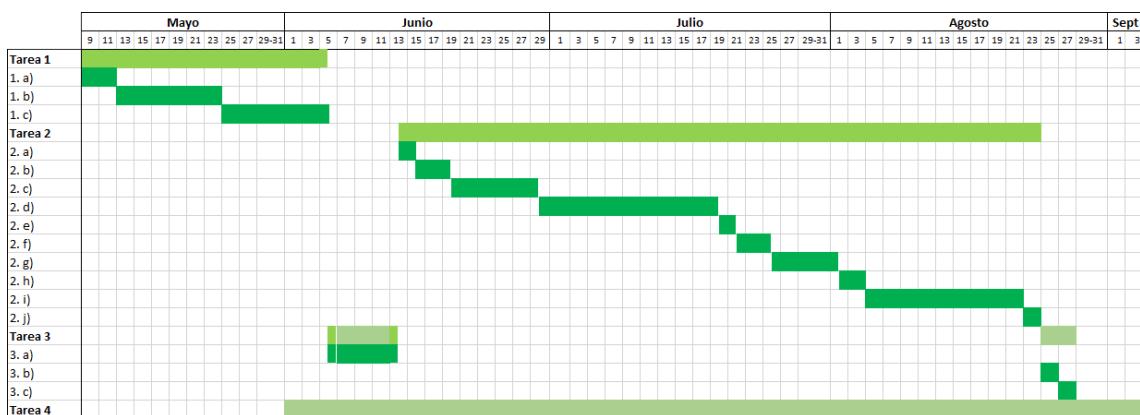
La planificación inicial del trabajo se puede revisar en 5.3. En la tabla 5.3 se puede revisar la planificación de las tareas definidas, con las fechas de realización de cada una de ellas. Además, en ?? se muestra un diagrama de Gantt el cuál representa los momentos de realización de cada tarea y su tiempo de duración.

B.3. Planificación final

En la siguiente tabla e imagen se puede ver la planificación final del proyecto.

Tabla B.1: Planificación final de tareas

Tarea	Días	Fecha de inicio	Fecha de fin
1. a)	8	9 de mayo	12 de mayo
1. b)	24	13 de mayo	24 de mayo
1. c)	16	25 de mayo	5 de junio
2. a)	2	14 de junio	15 de junio
2. b)	4	16 de junio	19 de junio
2. c)	10	20 de junio	29 de junio
2. d)	20	30 de junio	19 de julio
2. e)	2	20 de julio	21 de julio
2. f)	4	22 de julio	25 de julio
2. g)	6	26 de julio	31 de julio
2. h)	4	1 de agosto	4 de agosto
2. i)	18	5 de agosto	22 de agosto
2. j)	2	23 de agosto	24 de agosto
3. a)	8	6 de junio	13 de junio
3. b)	2	25 de agosto	26 de agosto
3. c)	2	27 de agosto	28 de agosto
4.	15	1 de junio	4 de septiembre

**Figura B.1:** Diagrama de Gantt con la planificación final de tareas