universidad de león

Departamento de Matemáticas

MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD

Trabajo de Fin de Máster

TÍTULO DEL TRABAJO

TITLE OF THE WORK

Autor: Nombre y apellidos del autor

Tutor: Nombre y apellidos del tutor

(Mes, Año)

UNIVERSIDAD DE LEÓN
Departamento de Matemáticas
MÁSTER UNIVERSITARIO EN INVESTIGACIÓN EN CIBERSEGURIDAD
Trabajo de Fin de Máster

ALUMNO: Nombre y apellidos del alumno

TUTOR: Nombre y apellidos del tutor

TÍTULO: Título del Trabajo Fin de Máster

TITLE: Title of the work

CONVOCATORIA: Mes, año

RESUMEN:

El resumen reflejará las ideas principales de cada una de las partes del Trabajo Fin de Máster pudiendo incluir un avance de los resultados obtenidos. Constará de un único párrafo y se recomienda una longitud no superior a 300 palabras. En cualquier caso esta Hoja de Datos no deberá superar una página de longitud.

Palabras clave: Lorem, ipsum, dolor, sit, amet..

Firma del alumno:	**VºBº Tutor:**

Índice general

Índice de figuras

Índice de tablas

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.

DES : Data Encryption Standard. Es un algoritmo criptográfico, de tipo cifrado por bloque.

Introducción

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 [1]. 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. A diferencia de NFC, la etiqueta RFID, se puede escanear a una distancia de hasta 100 centímetros [2]. 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).

Los dispositivos habilitados para NFC pueden comunicarse entre sí cuando se encuenftran 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 [3]. 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 [4]. 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 inciador 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.

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 pa-

ra 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 [5] 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) [6].

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.

Posibles amenazas

1. *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.

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.

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 extremo. 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.

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. La mejor manera de contrarrestar el ataque de inserción de datos es también el uso de un canal seguro para la comunicación.

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. 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

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 [7]. En este caso se impide el acceso

a información o servicios del usuario autorizado [8]. 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.

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.

c) 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. No deja de ser un modo de corrupción de datos.

Metodología

Estructura del trabajo

Ejemplos de uso de LaTeX (QUITAR DE LA MEMROIA)

Ejemplo de uso de notas al pie

El término *seguridad informática* abarca muchos aspectos, y dar una definición de manera genérica es complejo. Debe poderse aplicar a cualquier tipo de sistema informático, y al mismo tiempo describir qué se entiende por seguridad.

Aunque existen diferentes definiciones según la fuente, a continuación se presentan algunos enunciados concisos:

- "Es la protección de los datos, de las redes y del suministro eléctrico de un sistema informático."[1]
- "Disciplina que se ocupa de diseñar normas, procedimientos y técnicas, destinados a conseguir que un sistema de información sea seguro."[2]
- "Área de la informática enfocada en la protección de las infraestructuras computacionales y, especialmente, de la información contenida o que circula por ellas."[2]

Ejemplo de imagen

Existen tres requisitos fundamentales a tener en cuenta de cara a proteger la información que procesan los sistemas informáticos. Se trata de: *confidencialidad*,

[1] *Definition of computer security.* Encyclopedia. Ziff Davis, PCMag. `http://www.pcmag.com/encyclopedia/term/44958/information-security`

[2] `https://es.wikipedia.org/wiki/Seguridad_informática`

integridad y *disponibilidad*. Estos conceptos se refieren al uso, transferencia y almacenamiento de los datos, respectivamente.

En la figura 1 puede verse un esquema con los tres requisitos mencionados.

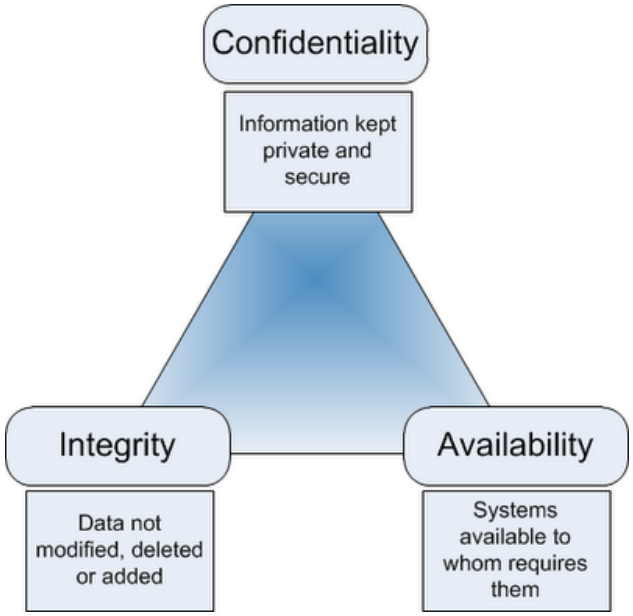

Figura 1: Elementos principales de seguridad de la información
Fuente: *http://geraintw.blogspot.com.es/2012/09/cia-infosec.html*

Ejemplo de lista con números

1. Confidencialidad:
   El principio de confidencialidad consiste en asegurar que la información es accesible sólo para aquellos destinatarios que estén autorizados, con independencia de dónde se almacene la información. La confidencialidad de los datos se implementa mediante mecanismos de control de acceso, tanto físicos (hardware) como de programación (software).

2. Integridad:
   La integridad de los datos se refiere a garantizar el estado de la información, protegiéndola de cambios accidentales o malintencionados. Mantener la integridad es esencial para la privacidad, la seguridad y la fiabilidad de los datos almacenados en un sistema. Las medidas que se utilizan para mitigar posibles fallos en los datos incluyen: copias de seguridad regulares, almacenamiento seguro de esas copias fuera del lugar de trabajo y herramientas de control de integridad.

3. Disponibilidad:
   La disponibilidad de los datos tiene como objetivo que los usuarios autorizados tengan acceso a la información en el momento que la necesiten. Esto implica garantizar el correcto funcionamiento de los equipos utilizados para almacenar y procesar los datos, de los controles de seguridad para protegerlos, y de los canales de comunicación utilizados para acceder a ellos.

Una tabla con varias cabeceras

La tabla 1 extiende a los robots sociales y asistenciales la clasificación de criticidad para sistemas industriales, propuesta en [24].

Tabla 1: Perfiles de seguridad asociados a la robótica

	Criticidad		
Perfil	Confidencialidad	Integridad	Disponibilidad
Estación de trabajo (PC)	Alta	Alta	Baja
Equipo para control industrial	Baja	Media	Muy alta
Robots asistenciales	Muy alta	Muy alta	Muy alta
Robots sociales	Muy alta	Media	Baja

Descripción de ROS: Robot Operating System

Vistazo general sobre ROS:
- Historia y versión actual.
- Aplicación: investigación y también robots comerciales.
- Arquitectura: componentes básicos y funcionamiento.

Ejemplo de código fuente

```
#!/bin/bash

# VARIABLES GLOBALES:

BASHRC_FILE="$HOME/.bashrc"
HOST_VAR_NAME="ROS_HOSTNAME"
```

```
7  MASTER_VAR_NAME="ROS_MASTER_URI"
8  ROS_PORT="11311"
9  HOST_IP=""    # Se asigna por parametro.
10 MASTER_IP=""  # Se asigna por parametro.
11 FILENAME="$(basename $0)"
12
13 # FUNCIONES:
14
15 description() {
16 if [ $1 -ne 0 ]; then
17 echo -e "\n ========="
18 fi
19 echo -e "\n  This script adds or modifies $HOST_VAR_NAME and $MASTER_VAR_NAME
       variables"
20 echo -e "    in the '~/.bashrc' file of current user.\n"
21 }
```

Capítulo 1

Estudio del problema

Se presenta el contexto de realización del trabajo realizando una revisión de las tecnologías, plataformas, herramientas o trabajos previos realizados en el mismo. Extensión aproximada de veinte páginas.

1.1. El contexto del problema

Breve descripción del contexto de realización del trabajo. Sirve para situar al lector.

1.2. El estado del arte

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 [9], así como la guía PRISMA [10].

1.2.1. Definición del proyecto

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 han considerado varias fuentes de información tales como IEEE Digital Library y Scopus.

Una vez decididas las bases de datos en las que se van a realozar las búsquedas, es necesario construir cadenas de búsqueda adecuadas que permitan obtener resultados satisfactorios. Para la realización de la búsqueda se han construido XXX 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.

Por otro lado se han realizado otras dos búsquedas separando las cadenas anteriores para conocer el estado de ambas tecnologías por separado dado que no hay una gran cantidad de artículos en la búsqueda anterior.

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

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.

1.3. 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

Capítulo 3

Estaciones de recarga del coche eléctrico (EVSE)

En la próxima década se espera un gran crecimiento de los vehículos eléctricos enchufables (PEV) 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 Equipo de Suministro de Vehículos Eléctricos (EVSE) o estaciones 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 de lPEV es la falta de una infraestructura de carga de PEV generalizada, a pesar de la gran difusión de la infraestructura eléctrica. Aunque se espera que el problema del coste de los PEV 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 rellenar el depósito de combustible de los vehículos de combustión interna [11], son percibidos actualmente por los compradores como serias barreras a la compra [12] [13].

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 PEV, 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 sistema ciberfísico. Estos sistemas ciberfísicos (CPS, por sus siglas en inglés) 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, deegación de servicio (DoS) y el malware se propaga del vehículo eléctrico o PEV al EVSE. El informe antes mencionado y algunos otros estudios [14] [15] [16] 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 PEV 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 PEV 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 PEV 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 PEV 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 PEV 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 PEV 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 PEV 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 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 PEV 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 PEV. 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 EVSE

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 usuario 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 iden-

tificador único del dispositivo (por ejemplo, el tag 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 tupo 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 PEV). 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 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 PEV-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 l 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 PEV 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. Estolo 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 dise;o 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 [17] [18] [22] [23] 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 [17]. 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 [18] 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. Estándar de protocolo de punto de recarga abierto (Open Charge Point Protocol, 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 PEV 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 PEV y los EVSE. Los principales estándares son [19] [20]:

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 [20] [21] 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 sistema de gestión de estaciones de carga (CSMS) y está diseñado para adaptarse a cualquier tipo de técnica de carga [21].

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 PEV 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 el 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 PEV (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 hablemos 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 PEV 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 PEV 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 del sistema

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 el Simple Object Access Protocol (Protocolo Simple de Acceso a Objetos, SOAP) o el JavaScript Object Notation (Notación de objetos de JavaScript, 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 PEV 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.

1. *Vehículo eléctrico*: El PEV 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 spartphone o tablet) o en algunos casos con un protocolo inalámbrico de amplio rango (por ejemplo, conexión 4G/5G) ya existente en

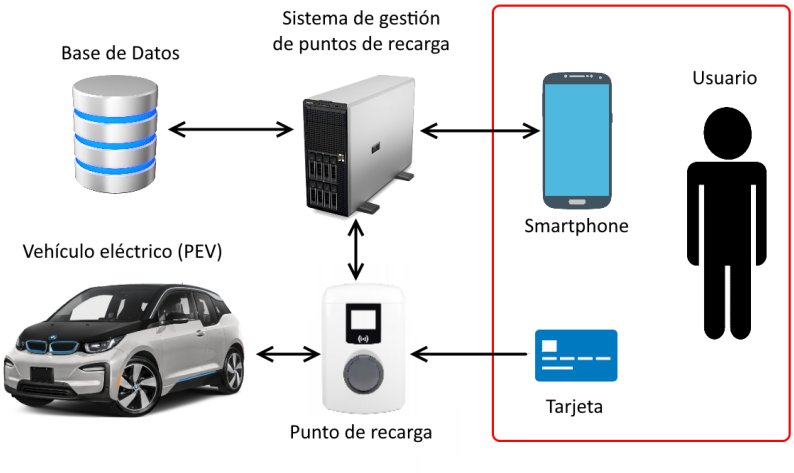

Figura 4.1: Arquitectura del sistema propuesto

el PEV. 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 PEV, 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. *Sistema de gestión de estaciones de carga (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 PEV 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:

Cuando un punto de recarga va a cargar a un PEV, 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 PEV 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:

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.

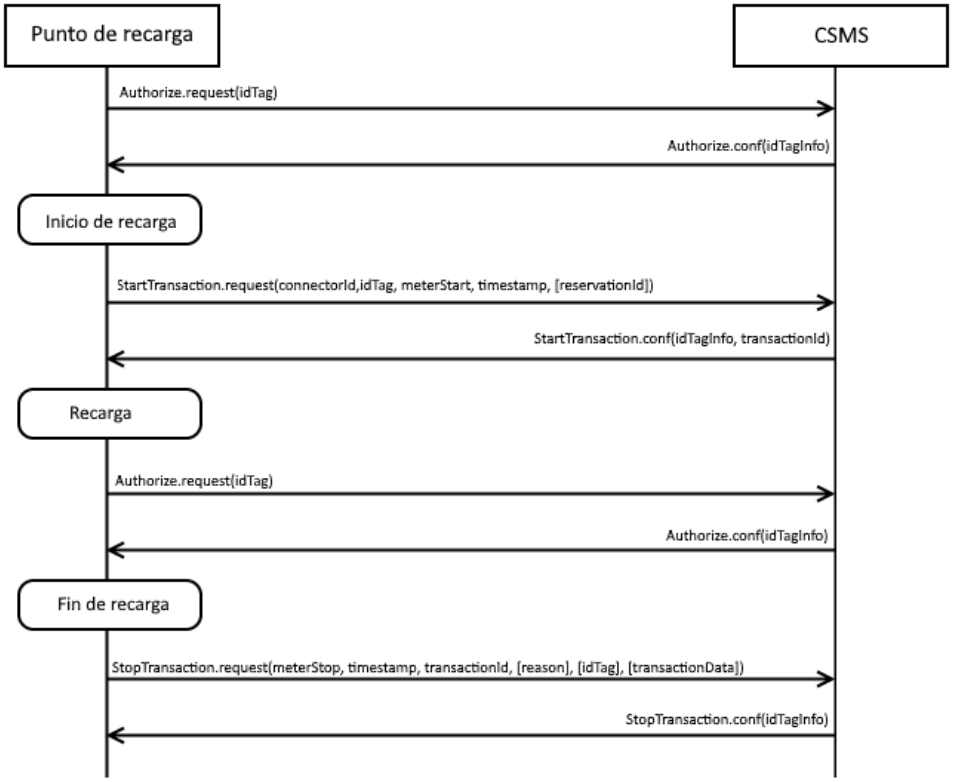

Figura 4.2: Diagrama de secuencia de una recarga

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 autorizacióny/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.

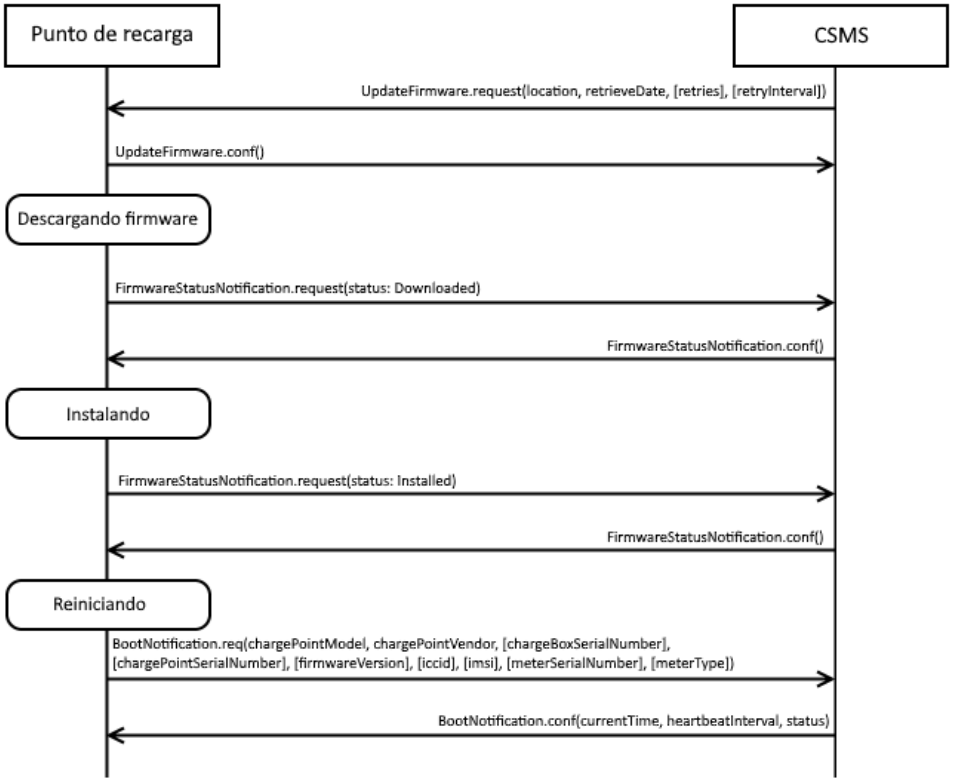

Figura 4.3: Diagrama de actualización de firmware

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 coincida 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)

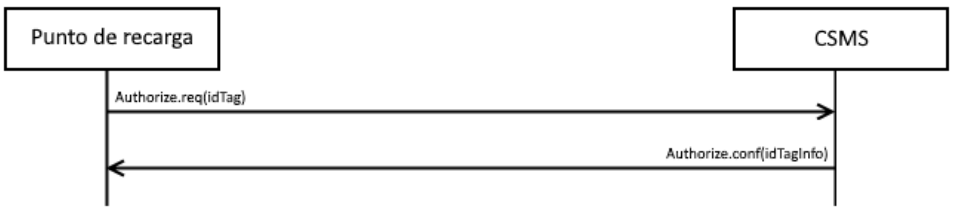

Figura 4.4: Diagrama de Authorize

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)

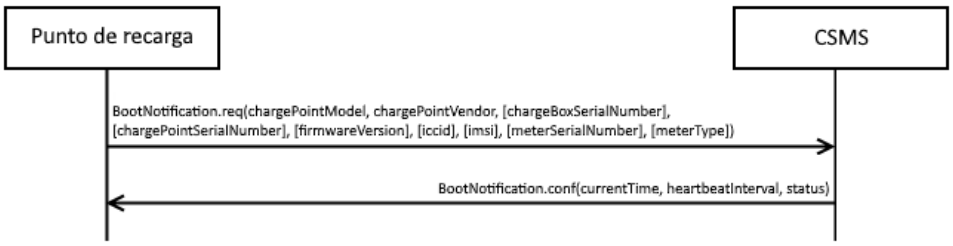

Figura 4.5: Diagrama de BootNotification

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 conexuón) 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 debría 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)

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.

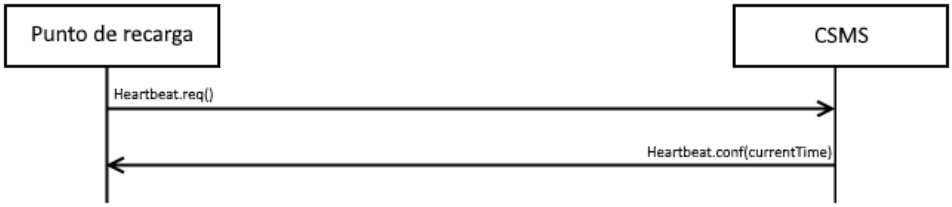

Figura 4.6: Diagrama de Heartbeat

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)

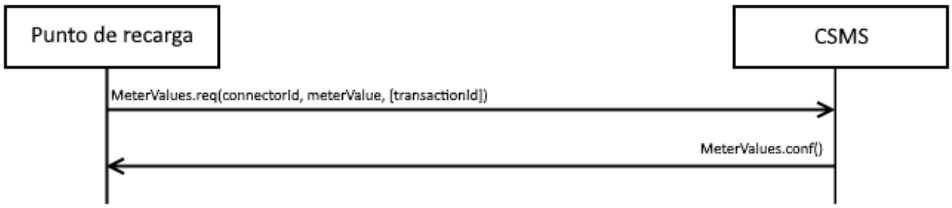

Figura 4.7: Diagrama de MeterValues

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 *ConectorId* 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 tios 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 PEV 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 campos opcionales 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 (watios 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)

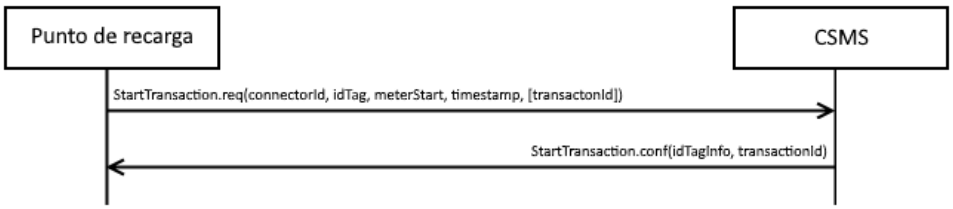

Figura 4.8: Diagrama de StartTransaction

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)

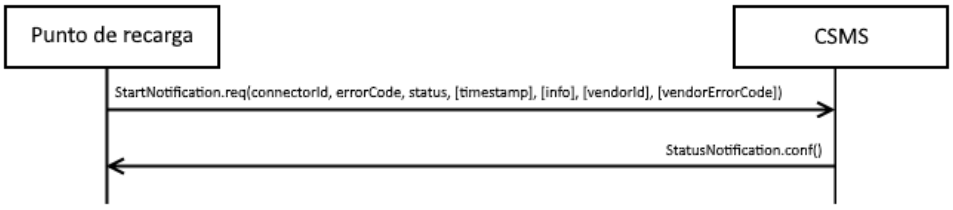

Figura 4.9: Diagrama de StatusNotification

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: my caption

-	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 *Reserve Now* (reservar ahora)
A8	Se recibe un mensaje *Change Availability* (cambio de disponibilidad) que marca el conector como *Unavailable*
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 consitente 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 *Unavailable*
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 *Unavailable*
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 *Unavailable*
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 *Unavailable*
F9	Se detecta un fallo que impide posteriores operaciones de carga
G1	La reserva caduca o se recibe un mensaje *Cancel Reservation* (cancelación de reserva)
G2	Se presenta la identidad de la reserva
G8	La reserva caduca o se recibe un mensaje *Cancel Reservation* (cancelación de reserva) y el conector está programado para ponerse en el estado *Unavailable*
G9	Se detecta un fallo que impide posteriores operaciones de carga
H1	El conector se configura como *Disponible* después de que llegase un mensaje *Change Availability* (cambiar disponibilidad)
H2	El conector se configura como *Disponible* después de que el usuario haya interactuado con el punto de recarga
H3	El conector se configura como *Disponible* 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 agregará 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 pPunto 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)

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-

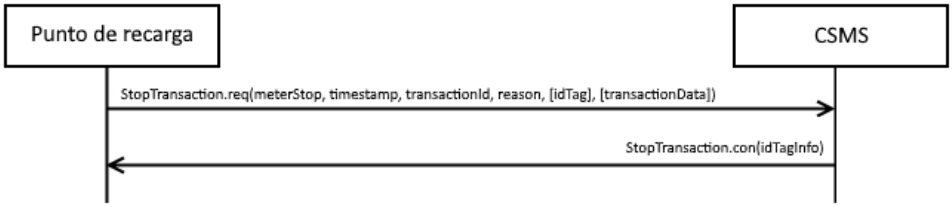

Figura 4.10: Diagrama de StopTransaction

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 PEV. 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 ún 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 elvalor *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)

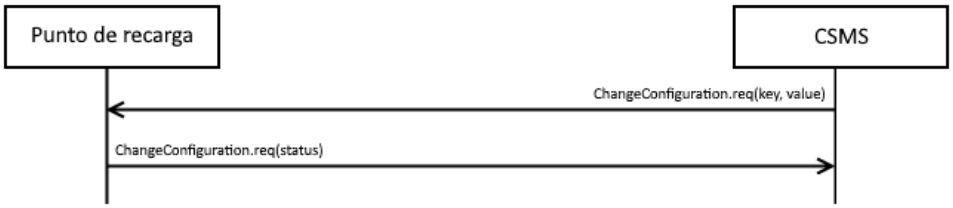

Figura 4.11: Diagrama de ChangeConfiguration

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)

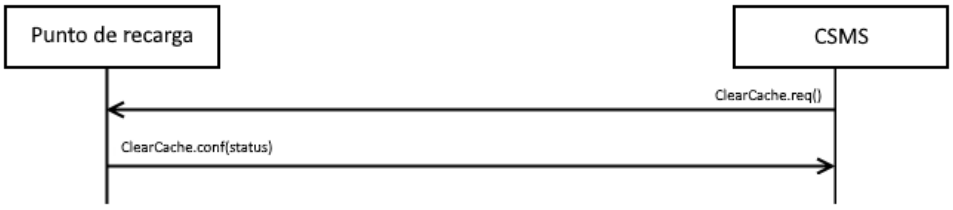

Figura 4.12: Diagrama de ClearCache

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.

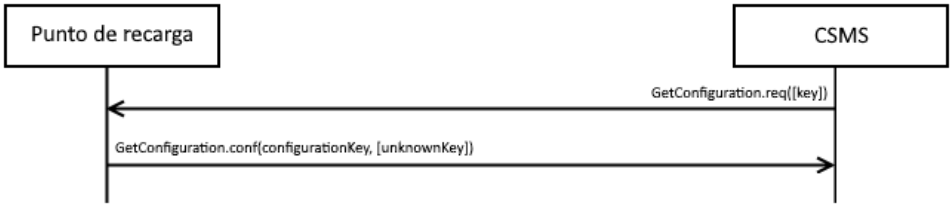

Figura 4.13: Diagrama de GetConfiguration

4.1.7.3. GetConfiguration (obtener configuración)

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)

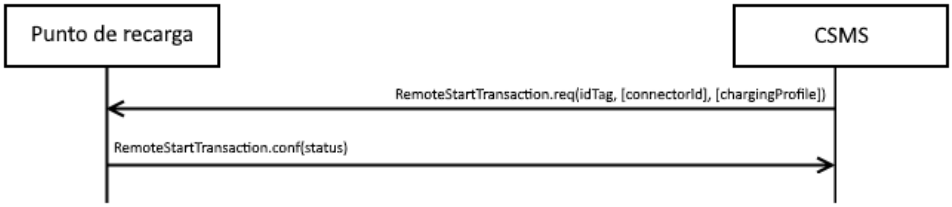

Figura 4.14: Diagrama de RemoteStartTransaction

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 SMSpara 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.

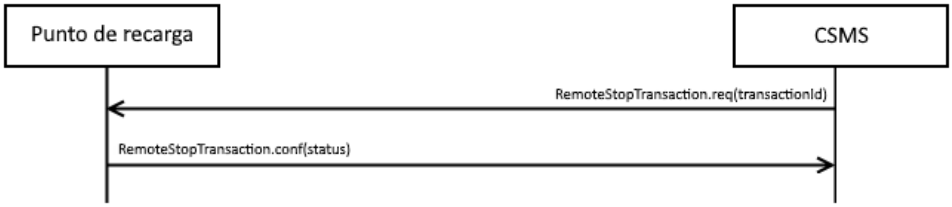

Figura 4.15: Diagrama de RemoteStopTransaction

4.1.7.5. RemoteStopTransaction (detención de recarga remoto)

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)

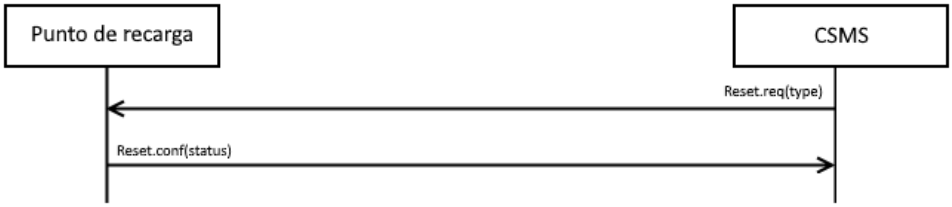

Figura 4.16: Diagrama de Reset

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 reincio.

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)

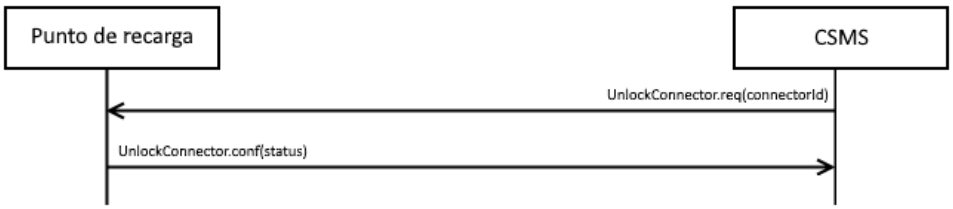

Figura 4.17: Diagrama de UnlockConnector

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 PEV 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

5.1.1. Definición del proyecto

5.1.2. Estimación de tareas y recursos

5.1.3. Presupuesto

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

5.1.3.1. Coste de personal

5.1.3.2. Coste del hardware

Para la realización de este proyecto se ha realizado la compra de:

1. Ordenador con Intel i7:

Tabla 5.1: Presupuesto de personal

Tarea	Perfil	Horas	Euros/Hora	Total
Desarrollo aplicación	Programador Junior	80	60	4800 €
Integración en entorno robótico	Programador Senior	20	100	2000 €
Pruebas	Ingeniero de Pruebas	20	80	1600 €
Supervisión del Proyecto	Jefe de Proyecto	10	120	1200 €
Total				10100 €

Placa base: MSI GE62 6QF-060ES Heroes Ed.

Procesador: Intel i7-6700HQ

RAM: 16 GB

Disco duro: 1TB + 128GB SSD

Tarjeta gráfica: Nvidia GTX970M

Monitor: 15.6"

- Precio (sin IVA): 986,71 €

2. Ordenador con Intel Atom:

   Asus Transformer Book H100TAM DK028B

   RAM: 32GB

   Disco duro: 500GB

   - Precio (sin IVA): 260,27 €

Tabla 5.2: Presupuesto total

Concepto	Coste (Euros)
Costes de personal	10100
Costes de hardware	1246,98
Subtotal	11346,97
IVA (21 %)	2882,86
Total Proyecto	**13729,83 €**

5.1.3.3. Coste total

5.2. Plan de trabajo

5.2.1. Identificación de tareas

5.2.2. Estimación de tareas

5.2.3. Planificación de tareas

5.3. Gestión de recursos

5.3.1. Especificación de recursos

5.3.2. Asignación de recursos

5.4. Gestión de riesgos

5.4.1. Identificación de riesgos

5.4.2. Análisis de riesgos

Capítulo 6

Solución

Explicación de la solución llevada a cabo. Si se trata de un desarrollo se incidirá en el proceso de desarrollo; en otro caso, se justificará y describirá la solución propuesta. El capítulo tendrá una extensión aproximada de cuarenta páginas y, en ningún caso, excederá las cincuenta.

6.1. Descripción de la solución

Breve descripción del tipo de solución adoptada: si es una aplicación y qué características tiene, si se trata de un tutorial, un modelo, etc.

6.2. El proceso de desarrollo

Explicar el modelo de proceso y la estructura de la sección.

6.2.1. 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 desccribirá 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 un tag 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*.

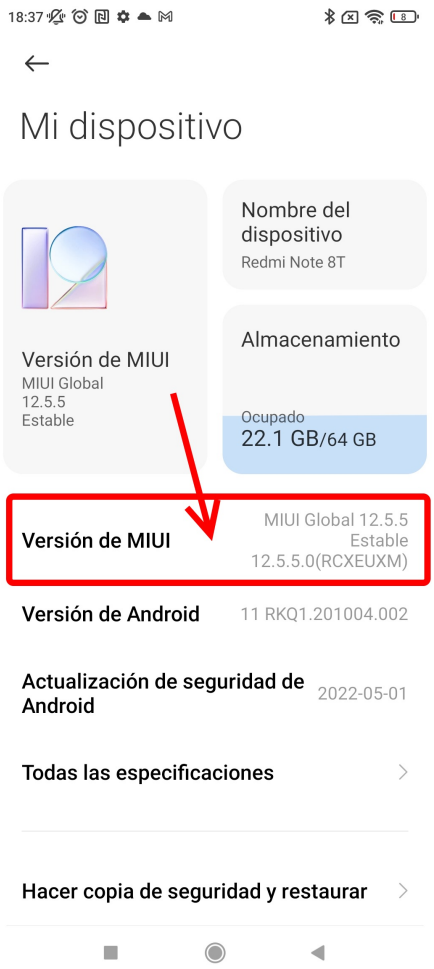

Figura 6.1: Pantalla de *Mi Dispositivo*

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.

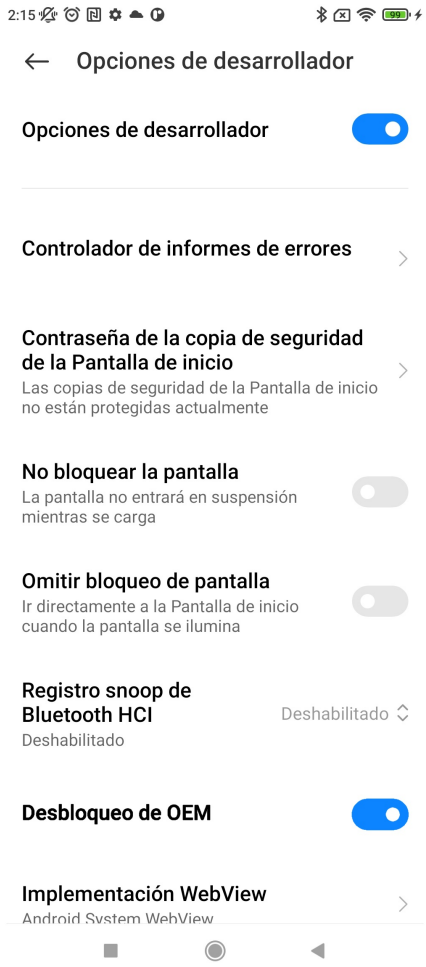

Figura 6.2: Pantalla de *Opciones de desarrollador*

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 iniciarlo en un modo llamado *fastboot*. Se conecta al ordenador y se espera que el botón *Unlock* se sitúe en verde.

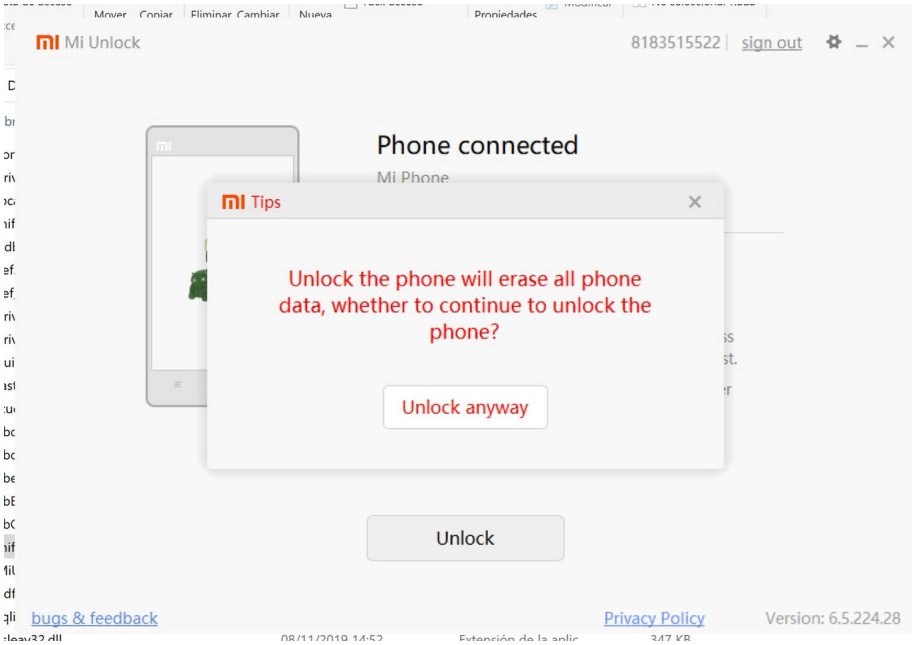

Figura 6.3: Pantalla de advertencia previa a desbloqueo de *Mi Unlock*

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).

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.

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

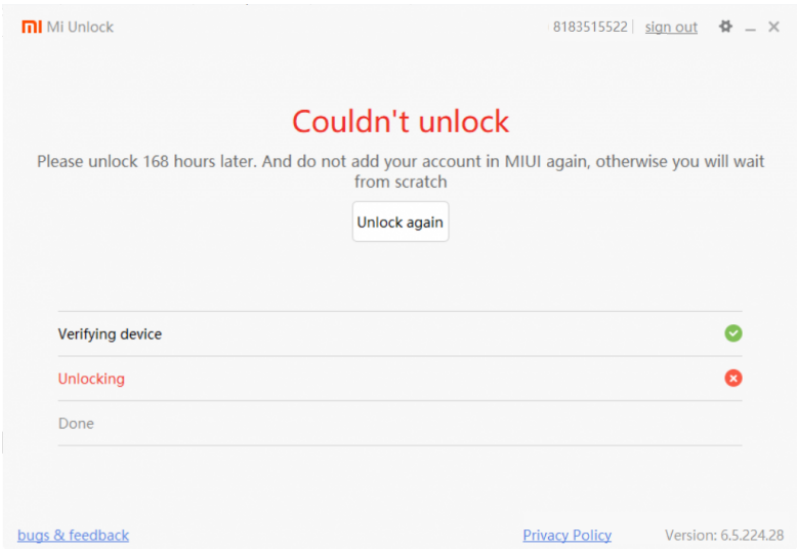

Figura 6.4: Pantalla de aviso de tiempo a esperar para desbloqueo de dispositivo mediante *Mi Unlock*

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.

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

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-Veritypor ese orden para poder rootear el dispositivo.

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

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

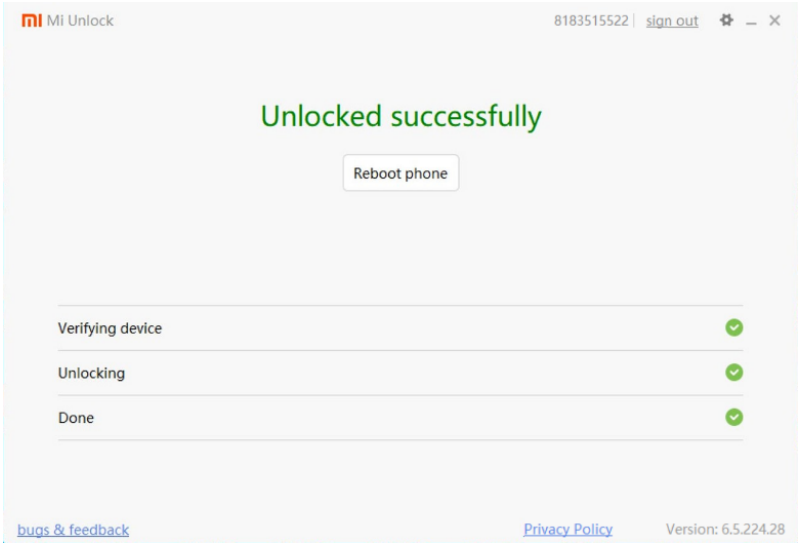

Figura 6.5: Pantalla de aviso de de dispositivo correcto en *Mi Unlock*

Desde la app se incica 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 del tag de la misma y se guarda en *Aceptar*.

Se pulsa en el icono 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 tag de la 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.

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.

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

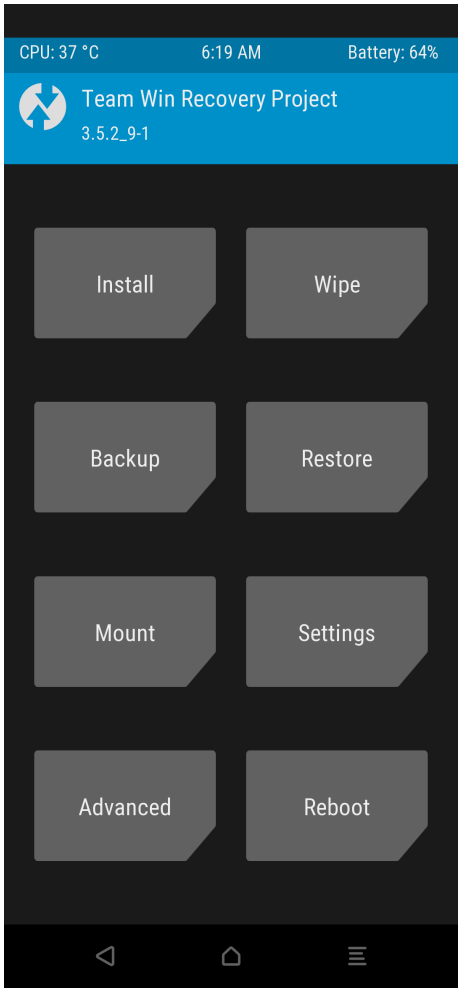

Figura 6.6: Pantalla principal de TWRP

6.2.2. Análisis

Fase de análisis

6.2.2.1. Definición de requisitos

Enumerar los requisitos del sistema dividiéndoles en funcionales y no funcionales.

6.2.2.2. Especificación de requisitos

Analizar y especificar los requisitos desde el punto de vista del comportamiento, estructura y funcionalidad del sistema.

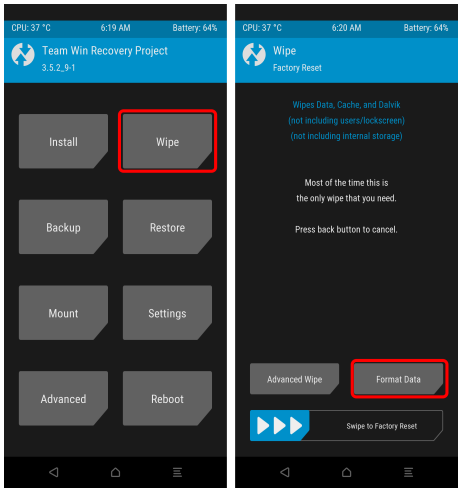

Figura 6.7: Proceso para formatear el dispositivo

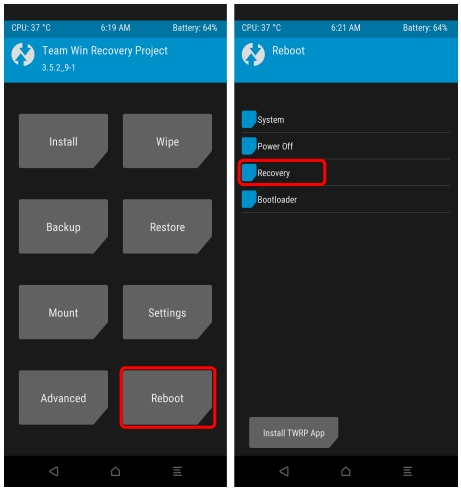

Figura 6.8: Proceso para reiniciar en modo recovery

6.2.3. Diseño

Fase de diseño

6.2.3.1. Diseño de sistema

Se expone la ARQUITECTURA del sistema y las TECNOLOGÍAS utilizadas en el desarrollo.

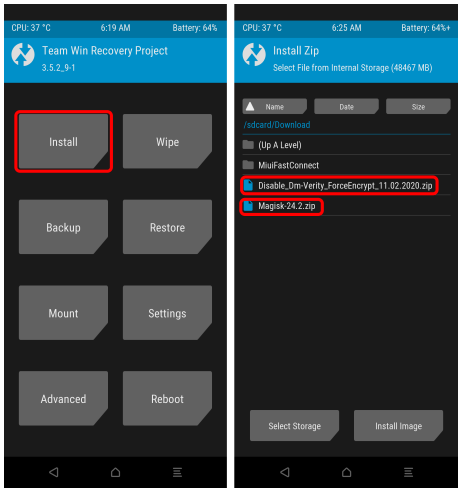

Figura 6.9: Proceso para instalar ficheros zip para rootear

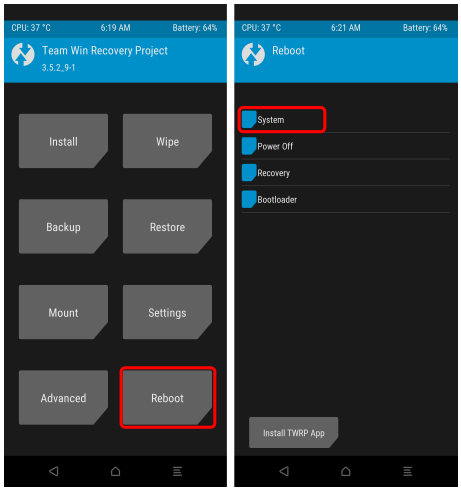

Figura 6.10: Proceso para inciar el móvil en funcionamiento normal

6.2.3.2. Diseño detallado

Se describe el diseño de las capas de PERSISTENCIA, MODELO e INTERFAZ del sistema.

6.2.4. Implementación

Hablar de las HERRAMIENTAS utilizadas durante el desarrollo, la ORGANIZACIÓN del proyecto y aquellas peculiaridades de la forma de implementación.

Figura 6.11: Pantalla de *Emulador de tarjetas Pro* tras instalar la app

6.2.5. Pruebas

Centrarse en pruebas unitarias (no incluir todas las pruebas sino informes de las mismas) y de sistema (mostrar que cumple los casos de uso).

6.3. El producto del desarrollo

En el caso de desarrollar una herramienta es necesario mostrar, brevemente, el tipo de herramienta generada. Incluir algún pantallazo de la herramienta, su funcionalidad y la forma de ejecución de la misma.

Figura 6.12: Pantalla de *Emulador de tarjetas Pro* tras leer una tarjeta

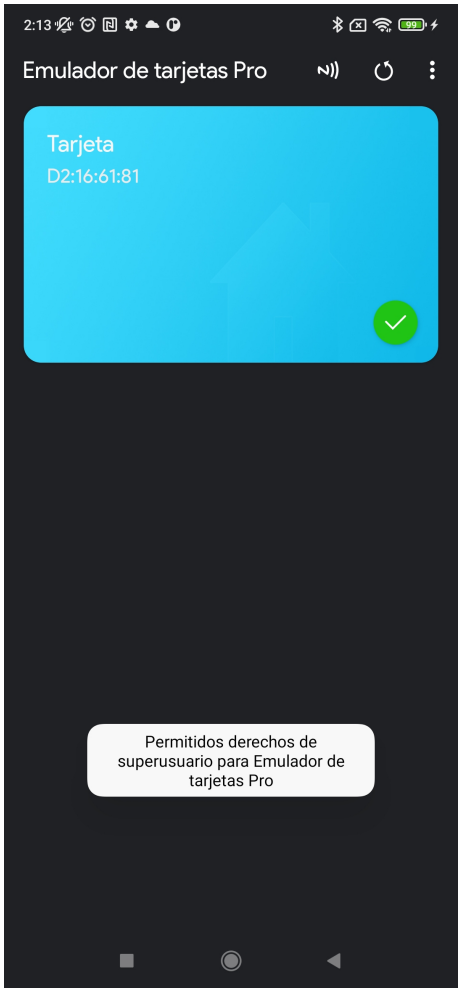

Figura 6.13: Pantalla de *Emulador de tarjetas Pro* durante la emulación de una tarjeta

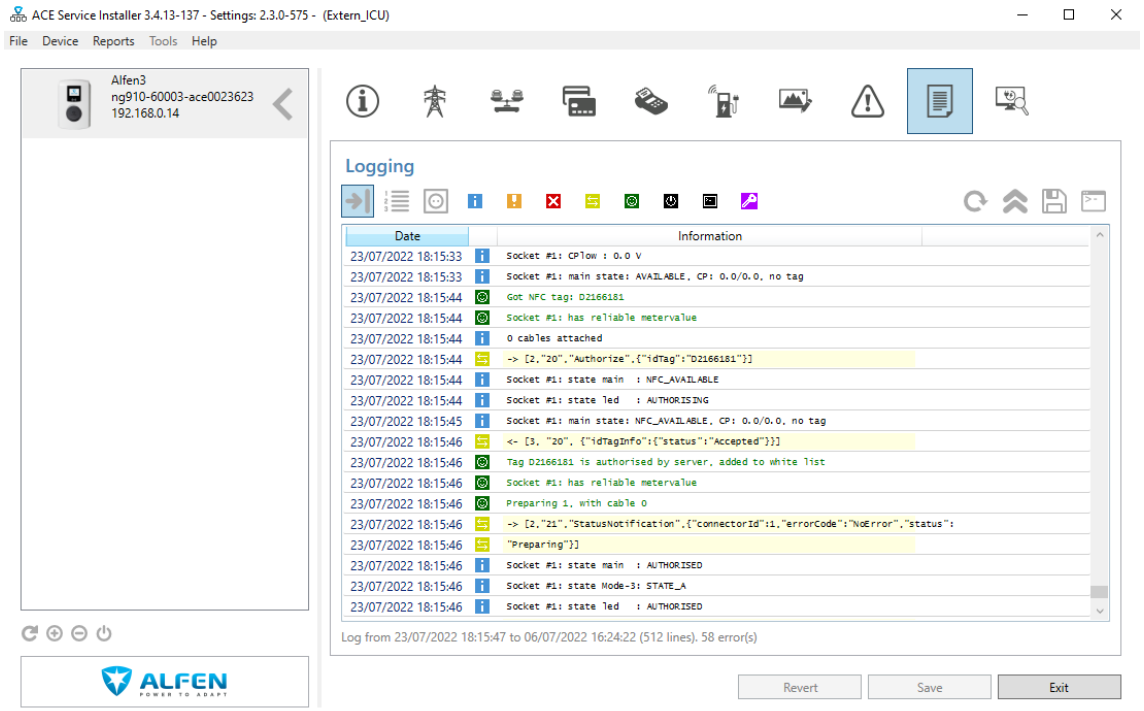

Figura 6.14: Pantalla de logs de *Ace Service Installer* tras el paso de tarjeta

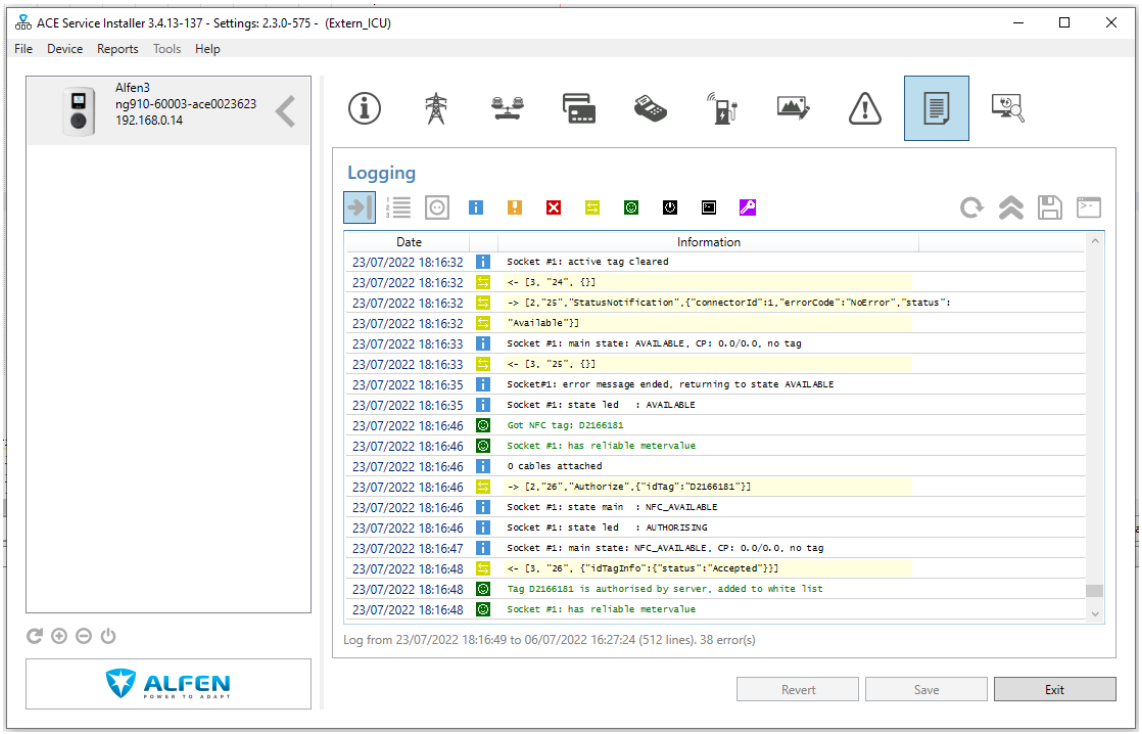

Figura 6.15: Pantalla de logs de *Ace Service Installer* tras el paso del smartphone que simula la tarjeta

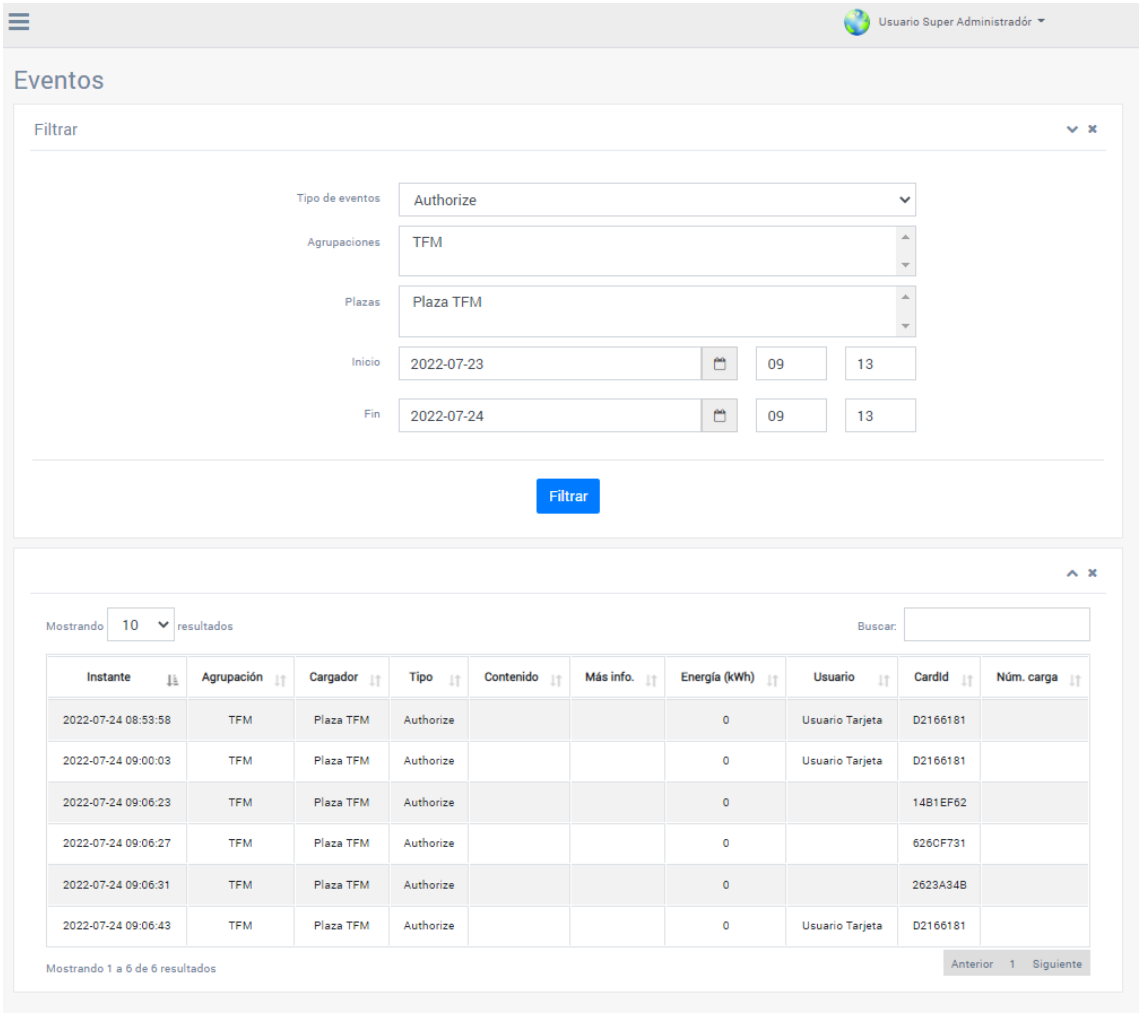

Figura 6.16: Pantalla de eventos de la web tras los pasos de los tags

Capítulo 7

Evaluación

Demostración de la validez de la solución elaborada. La solución se considera válida si resuelve los problemas expuestos en el planteamiento del problema y satisface los objetivos definidos en la introducción. Según el caso la forma de evaluación se basará en la ejecución de casos de prueba o en la realización de cuestionarios. Extensión entre quince y veinte páginas.

7.1. Proceso de evaluación

7.1.1. Forma de evaluación

Explicar la forma en la cual se ha evaluado la aplicación

7.1.2. Casos de prueba

Casos de pruebas realizados

7.2. Análisis de resultados

Conclusión

Expresión personal del conjunto de conclusiones que, a juicio del autor, se derivan de los resultados expuestos en el trabajo.Deberá tener una extensión entre cinco y diez páginas.

Aportaciones realizadas

Trabajos futuros

Problemas encontrados

Opiniones personales

Información bibliográfica citada en el texto del trabajo. Otras lecturas recomendadas o consultadas, de figurar, aparecerán en anexos. Se debe seguir la norma ISO 690 (buscar en google ISO 690 ugr)

Lista de referencias

[1] *P*. V. Nikitin, K. V. S. Rao y S. Lazar, "An overview of near field UHF RFID", IEEE RFID. Conferencia, 2007, págs.167-174.

[2] *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.

[3] *I*SO/IEC 18092. "Near Field Comunication: interface and protocolo", 2004.

[4] *E*CMA International (2005). "Near Field Communication - White Paper", Ecma/TC32-TG19/2005/ 012, 2005.

[5] ''NFC Data Exchange Format (NDEF), NFC Forum Technical Specification"

[6] ''NFC-Near Field Communication, Reader/Writer Operating Mode"

[7] *F*ahrianto 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

[8] *E*un 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

[9] *K*itchenham, B.A., Budgen, D., Brereton, P. "Evidence-Based Software Engineering and Systematic Reviews", vol. 4. CRC Press (2016)

[10] *M*oher, 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.

[11] *S*aalfeld, C. "E-Mobility–Vehicle2Grid Interface. Vector-Kongress", 2010

[12] *B*edogni, 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.

[13] *B*edogni, 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.

[14] *R*hode, K. "Electric Vehicle Cyber Research SANS Automotive Cybersecurity Workshop", 2017

[15] *S*hezaf, O., "Who can hack a plug? The Infosec Risks of Charging Electric Cars", 2013.

[16] *F*earn, F. Kaspersky, V3 news, "Warning over electric car charging", Enero de 2018.

[17] *K*ocher, 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.

[18] *K*helladi, Lyes, et al. "On security issues in embedded systems: challenges and solutions." International Journal of Information and Computer Security 2.2, 2008.

[19] *B*uamod 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.

[20] *S*chmutzler J., Andersen C.A., Wietfeld C., "Evaluation of OCPP and IEC 61850 for smart charging electric vehicles". World Electr. Veh. J., 2013

[21] *H*ome - Open Charge Alliance. Web: https://www.openchargealliance.org/.

[22] *W*an, Kaiyu, K. L. Man, y D. Hughes. "Specification, Analyzing Challenges and Approaches for Cyber-Physical Systems (CPS)." Engineering Letters 18.3, 2010.

[23] *O*rojloo, Hamed, y Mohammad Abdollahi Azgomi. "A method for modeling and evaluation of the security of cyber-physical systems." Information Security and Cryptology (ISCISC), 11ª Conferencia Internacional ISC sobre IEEE, 2014.

[24] CSSP, D.: *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies.* US-CERT Defense In Depth. (Octubre 2009)

Anexo A

Control de versiones

Anexo B

Seguimiento de proyecto fin de máster

Obligatorio. Seguimiento del trabajo real.

B.1. Forma de seguimiento

B.2. Planificación inicial

B.3. Planificación final

Si el trabajo ha consistido en la elaboración de una aplicación se incluirá el manual de usuario de la misma.

Anexo C

Cuestionario de evaluación

Cuestionarios utilizados durante la fase de evaluación.