C. Alcaraz, A. Garcia, and J. Lopez, "Implicaciones de seguridad en MAS Desplegados en Infraestructuras de Carga basadas en OCPP", *VII Jornadas Nacionales en Investigación en Ciberseguridad (JNIC 2022)*, pp. 172-179, 2022.
NICS Lab. Publications: `https://www.nics.uma.es/publications`

Implicaciones de seguridad en MAS Desplegados en Infraestructuras de Carga basadas en OCPP

Cristina Alcaraz, Alberto Garcia y Javier Lopez

Computer Science Department, University of Malaga,

Campus de Teatinos s/n, 29071, Malaga, Spain

{alcaraz, albertogr, jlm}@lcc.uma.es

Resumen

El interés actual por desplegar infraestructuras de carga de vehículos eléctricos para el ahorro energético y la sostenibilidad es cada vez más palpable, lo que llama la atención a muchas comunidades, especialmente a la científica, para explorar, entre otras cosas, la influencia de las nuevas tecnologías de información en los procesos operacionales. Teniendo en cuenta este escenario, este artículo, por tanto, analiza cómo el uso de los sistemas de multi-agente pueden beneficiar las tareas de monitorización, mantenimiento y de seguridad, y propone una arquitectura específica en base a los actores especificados en el protocolo OCPP (Open Charge Point Protocol). Esta arquitectura constituye la base para analizar los diversos tipos de amenazas que agentes software pueden sufrir, clasificándolas de acuerdo a las características funcionales e interacciones con los diversos elementos de la infraestructura. Esta agrupación y el conjunto de ataques abordados están basados en el SP-800-19 definido por el National Institute of Standards and Technology, y formalizados siguiendo la metodología de árboles de ataque. El estudio revela la importancia que tiene analizar los riesgos que esta tecnología puede traer a este escenario, proporcionando, además, un conjunto de recomendaciones que sirvan de guía para aplicaciones futuras.

Keywords: Ciberseguridad infraestructuras de carga de vehículos eléctricos sistemas multi-agente, árboles de ataques

Tipo de contribución: *Investigación original*

1. Introducción

La evolución que está viviendo el sector de la movilidad está motivada entre otras cosas por la concienciación ecológica que cala cada vez más en la sociedad debido a la necesidad de sustituir las tradicionales fuentes de energía por otras con un menor impacto en el medio ambiente. Esto se refleja en el crecimiento del mercado de vehículos eléctricos, en el que se espera un volumen de crecimiento anual de 21,7 % para alcanzar 233,9 millones de unidades y los 2.495,4 millones de dólares para el año 2027 [1]. Esta demanda obliga a desplegar infraestructuras de carga tanto públicas como privadas,

que sostengan este nuevo modelo de transporte. Uno de los protocolos más extendido actualmente para dar soporte a este tipo de infraestructura es el protocolo OCPP (Open Charge Point Protocol) [2], el cual define un conjunto de actores y una arquitectura base en la que estaciones de carga se conectan a sistemas centralizados a cargo de la gestión y el control del suministro de energía, ofreciendo un conjunto de servicios específicos para la autorización de transacciones, gestión y configuración dinámica de las estaciones, mecanismos para reservar energía y diagnóstico. Aprovechando estos recursos fundamentales para diseñar y desplegar infraestructuras de carga, este artículo propone la aplicación de un sistema multi-agente (Multi-Agent System (MAS)) para tratar y optimizar aún más algunas de las implicaciones en materia de operación, mantenimiento y seguridad de infraestructuras de carga. Con esto, además, nos acercamos a la concepción idónea de interconectar Tecnologías de la Información (TI) con las Tecnologías Operacionales (TO) para beneficiar las operaciones en tiempo real y el modelo de negocio.

Para hacer una revisión del estado del arte, en el trabajo [3] se aborda un conjunto de problemas presentes actualmente en las estaciones de carga y propone el uso de la IA (Inteligencia Artificial) y tecnología blockchain para solventarlos, pero no estudia la aplicación y las implicaciones que tiene las nuevas TI tal como se aborda en este artículo. Por otro lado, algunos autores ya han llevado a cabo estudios previos sobre la utilización de agentes en redes de carga de vehículos eléctricos. Por ejemplo, en [4] se desarrolla un simulador basado en un MAS para analizar el comportamiento de los usuarios dentro de una red de cargadores. Su objetivo es determinar de forma óptima dónde desplegar las estaciones de carga para satisfacer la demanda. En [5], se diseña un MAS que tiene como función gestionar el consumo de los usuarios para minimizar el impacto en la red eléctrica. También simula el sistema planteando cuatro escenarios distintos para verificar su eficacia. El mismo objetivo se persigue en [6], en la que, además, se define una estructura jerárquica que mejora la planificación, y en [7] y [8] se realizan predicciones del comportamiento de los usuarios teniendo en cuenta factores sociales. Sin embargo, en todos estos trabajos, los agentes software (SW) se usan principalmente para la simulación y la planificación, no para desplegarlos junto a la red de carga como si fuese una red de monitorización secundaria, además de que no exploran al detalle las implicaciones que tiene el despliegue de dichos agentes desde el plano de la seguridad.

El presente artículo da un salto y propone, por un lado, una infraestructura de carga basada en un MAS para garantizar una monitorización constante de las estaciones de carga, midiendo estados de salud para contribuir con el mantenimiento predictivo y a la detección de amenazas, además de cumplir con el esquema estandarizado de interconexión del protocolo OCPP. Por otro lado, y en base a esta arquitectura, (i) se identifica y clasifica tipos de amenazas al sistema propuesto y de acuerdo al SP 800-19 definido por el National Institute of Standards and Technology (NIST) en [9], (ii) se formaliza y prioriza algunos ataques siguiendo la metodología de árboles de ataques, y (iii) se proporciona recomendaciones de seguridad como guía para implementar soluciones TI-TO seguras en el escenario propuesto.

El resto del artículo queda estructurado como sigue: en la sección 2 se presenta la arquitectura específica basada en OCPP y se introducen los agentes. En la sección 3 se clasifican las amenazas siguiendo la SP-800-19. Esta clasificación se complementa con

la aplicación de la metodología de modelado de amenazas con árboles de ataque en la sección 4. Más tarde, en la sección 5, se exponen algunas recomendaciones, con el fin de reforzar la seguridad en este escenario. Por último, las conclusiones de este estudio se recogen en la sección 6, junto con algunos detalles del trabajo futuro.

2. Despliegue de un MAS en redes de carga

Como se indica en la introducción, el escenario considerado en este trabajo consiste en una infraestructura basada en estaciones de carga (comúnmente conocidos como cargadores eléctricos) para vehículos eléctricos, y por el que hace uso del protocolo OCPP detallado en [2] y definido por el Open Charge Alliance. El protocolo considera los fundamentos tradicionales de cliente-servidor y de los principios de control entre las estaciones de carga y el sistema central, e incluye instrucciones de comando y control (C&C) necesarias para permitir que sistemas de control puedan gestionar y autorizar las recargas deseadas y diagnosticar en tiempo real las estaciones. Esta forma de conectar estaciones con sistemas de control, y de una manera estandarizada, ha llamado la atención a muchas manufactureras (ej. ABB, Schneider Electric, GARO, hypercharger, Legrand y efacec, entre otros), convirtiéndolo en un estándar de facto fuertemente apoyado por la industria [10]. Es tanta su influencia, que actualmente se encuentra disponible la versión OCPP 2.0.1 [2] que aborda los siguientes actores de interés también para nuestro estudio:

- CS (*Charging Station*): es el sistema ciber-físico, a través del cual, los usuarios de la infraestructura de carga pueden recargar sus respectivos vehículos eléctricos. Por tanto, una CS es la interfaz principal entre el usuario y la red de carga, cuyos elementos lo conforman: un controlador encargado de gestionar los sensores y actuadores integrados en su propia estación, además de incluir un contador inteligente para contabilizar el consumo eléctrico.

- CSMS (*Charging Station Management System*): está encargado de gestionar, supervisar y controlar las CS existentes en la red de carga. Procesa las peticiones de los usuarios que quieren hacer uso de los servicios de carga y se comunica con las CS involucradas para controlar la transacción de energía.

- EVSE (*Electric Vehicle Supply Equipment*): es el componente de la CS que aporta energía al vehículo. Cada CS puede contener uno o más EVSE, y cada uno es gestionado de forma independiente por la CS. En este trabajo se usa el concepto de redes de CS y redes EVSE de forma intercambiable.

- CSO (*Charging Station Operator*): entidad encargada de la administración y el mantenimiento de la red EVSE. Suele hacer referencia a una persona empleada para dichas tareas de gestión y control local.

- EMS (*Energy Management System*): dispositivo que controla la producción y el consumo real de energía de forma local o por áreas, según las políticas y normativas pre-establecidas. Para este control, se requiere, además, que el EMS

guarde estrecha relación y comunicación con el CSMS para producir y distribuir la energía de acuerdo a la demanda real.

- EV (*Electric Vehicle*): corresponde con el destinatario principal de la energía, cuando el usuario, dueño del EV, hace uso de los servicios de carga. En este punto, merece la pena destacar que un EV puede también actuar como fuente móvil de energía hacia la red eléctrica (en base a una comunicación y flujo de energía bidireccionales). Estos casos son definidos como V2G (Vehicle-to-grid).
- Infraestructura de tarificación: es la entidad encargada de establecer los precios, registrar la deuda y realizar el cobro por los servicios de carga ofrecidos a los usuarios.

El protocolo OCPP está diseñado para integrar prácticamente cualquier técnica comúnmente usada en el sector, soportando diversos métodos de autorización de usuarios: mediante tarjetas RFID, usando tarjetas de crédito, autorización remota a través del CSMS, etc. También contempla la posibilidad de que la CS pierda, de forma temporal, la conexión con el CSMS, pasando a operar en un estado "ofline" en el que la CS es capaz de gestionar de forma local una lista de autorización obtenida previamente del CSMS. Si no dispone de tal lista, la CS aceptará a cualquier usuario, por motivos de continuidad del negocio, para realizar la autenticación una vez que se haya recuperado la conexión con el CSMS y así poder tarificar y cobrar el servicio. Además, OCPP plantea tanto situaciones en las que el inicio de la transacción de energía es solicitado por la CS, como situaciones en las el CSMS inicia el proceso de carga ("remote control"). Otra de las características que implementa OCPP 2.0.1 es la posibilidad de reservar una CS (o bien un EVSE de la CS) con un período de antelación, de forma que ningún otro usuario pueda usarla durante ese tiempo.

2.1. El rol de los agentes software en CS

Dentro de la arquitectura propuesta, un conjunto de agentes SW se distribuyen en cada componente principal del sistema de carga (ya sea en la CS y el CSMS) con objeto de recolectar localmente y de manera dinámica información relevante que puede ayudar a mejorar las funciones primarias de cada estación y que puede ser vital para analizar el estado de salud de una red, favoreciendo, a su vez, las decisiones a realizar en los respectivos sistemas de CSMS y EMS. Además, estos agentes pueden tener la capacidad para compartir información que puede ser útil para intensificar aún más la "consciencia situacional", y explicar de primera mano: (i) qué ocurre dentro de un punto de carga y en qué momento determinado, además de (ii) identificar qué elementos hardware, software y red son afectados dentro de una CS, y (iii) qué vecinos pueden también estar implicados. Esta característica esta representada en la figura 1, donde podemos ver cómo las CS se pueden comunicar con el CSMS a través del protocolo OCPP, mientras una red paralela se despliega con respecto a la red de OCPP para contribuir en mejorar la calidad de los recursos de control frente a posibles fallos imprevistos o ataques inesperados, muchos de los cuales pueden provenir de insiders (ej. CSO con intenciones maliciosas) u outsiders (ej. el público general con acceso a las CS,

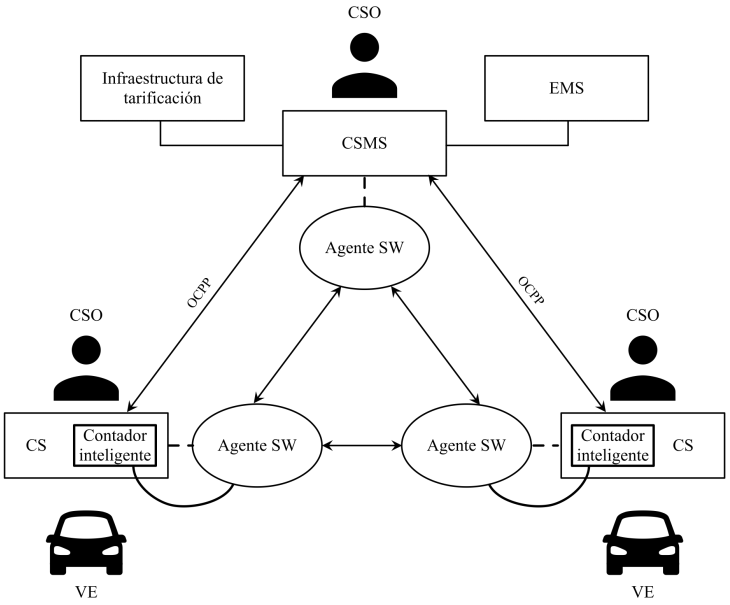

Figura 1: Inclusión del MAS a la red de carga

o terceros/proveedores de servicios HW o SW) con intereses para manipular valores relevantes de componentes CS [11, 12], e impactar consecuentemente en el suministro de energía y/o dañar el modelo de negocio y su cadena de valor.

En nuestro escenario, se consideran fundamentalmente dos roles distintos en función de (i) las tareas de las que se encarga, de (ii) la información que gestiona y de (iii) dónde se sitúe en la red de carga. Cada CS es la plataforma en la que se hospeda un agente SW que aquí llamamos *agente de monitorización*, ya que su función principal será la de obtener información local relativa al consumo de energía de la estación y su funcionamiento interno (recursos HW y SW disponibles, estado de los canales de comunicación con otros nodos de la red, tráfico de red, etc.), y en definitiva el estado de salud de la CS. Para conocer información referente al consumo (metering), este agente tiene acceso al contador local de la CS, con esto se consigue una doble verificación del consumo eléctrico (a través de los reportes del protocolo OCPP y del sistema MAS), mientras que se consigue un diagnóstico más completo. Por otro lado, el CSMS implementará su propio agente SW con un rol distinto al de los anteriores, al que denominamos *agente colector*. La inclusión de este agente permite recolectar la información obtenida por los agentes de monitorización presentes en todas las CS de la red, por lo que tiene un rol fundamental en la monitorización, diagnóstico y detección de amenazas en toda la infraestructura de carga. Aparte de esto, los recolectores pueden tener la capacidad de liderar funciones específicas de control (ej. interrumpir la toma de medición por los agentes de monitorización, solicitar datos de diagnóstico o cambiar de manera remota valores de configuración) y respuesta frente a incidentes.

Aplicando el enfoque MAS, mejoramos la capacidad de conocer con mayor detalle el estado de toda la red, reforzando la monitorización ofrecida por los tradicionales IDS/IPS (Intrustion Detection/Prevention Systems), SIEM (Security Information and Event Management), SOC (Security Operation Center) y firewalls, permitiendo tener una prevención y/o detección más temprana frente ataques específicamente diseñados para estos tipos sistemas ciber-físicos. Por otro lado, el uso de los agentes para comandar acciones de respuesta frente a amenazas potenciales del estilo APT (Advanced Persistent Attacks) contra las CS, permite al CSO tener un mayor control sobre la red y flexibilidad a la hora de elaborar planes de mitigación y recuperación.

Pese a esto, la incorporación del MAS debe realizarse con sumo cuidado, mirando especialmente en ciertos aspectos relacionados con la seguridad, de lo contrario se estarían introduciendo nuevas amenazas con nuevos patrones o vectores de ataque que pueden ser aprovechados por adversarios. Esto se debe a que los agentes no dejan de ser componentes SW que, si no son protegidos correctamente frente accesos no autorizados, son fácilmente manipulables por actores maliciosos. Esta connotación software añade además, la necesidad de precisar en los procesos de validación de códigos fuentes desde que éstos pueden presentar serios bugs que pueden ser fácilmente explotables por atacantes. Estos errores software puede incluso provenir de frameworks, librerías y herramientas proporcionadas por terceros, lo que conlleva a numerosos agujeros de seguridad. Por tanto, las siguientes secciones, exploran clases de amenazas a estos tipos de agentes SW (monitorización y recolectores), agrupándolos de acuerdo a sus interacciones.

3. Clasificación de amenazas de seguridad

Aunque existen metodologías efectivas para clasificar tipos de amenazas en sistemas basados en agentes software, como puede ser el tradicional modelo CIA (Confidentiality, Integrity and Availability), nosotros seguimos la metodología propuesta por el SP (Special Publication) 800-19, titulada "*Mobile agent security*" y definida por el NIST en [9]. Según este SP es posible clasificar las amenazas contra agentes software teniendo presente sus principales componentes así como sus relaciones, para luego categorizar las amenazas e identificar los posibles vectores de ataque. Por tanto, en las siguientes subsecciones vamos a analizar las interacciones que tienen los agentes con cada elemento de la infraestructura de carga, para posteriormente extraer posibles tipos de ataques en la siguiente sección.

3.1. Clase 1: agentes SW y las estaciones de carga (CS)

La estación de carga es el principal actor y componente ciber-físico en donde agentes software pueden desplegarse para la monitorización constante de los recursos de la CS, y, por lo tanto, el componente por el cual se espera que agentes puedan funcionar durante todo su ciclo de vida. Esto también significa que tanto una CS como un agente SW guardan una estrecha relación entre ellos, y esto, a su vez, es lo que conduce a establecer una categoría de amenazas en el que se incluyen todas aquellas que pueden poner en riesgo el bienestar y la seguridad de la CS. Por ejemplo, agentes SW mali-

ciosos o “rogue” (supuestos agentes legítimos del sistema) podrían ser integrados para intencionadamente impactar en el comportamiento de la CS, alterar datos de telemetría o de medición, violar operaciones críticas o corromper servicios esenciales.

Dicho de otro modo, el perfil de un agente malicioso dentro esta categoría consiste en una pieza de código con autonomía suficiente y privilegios para: (i) realizar tareas de gestión de archivos de registros, (ii) medir variables relativas al funcionamiento y al rendimiento de la CS, y (iii) ejecutar comandos C&C para la dar respuesta a incidentes de seguridad. Esta forma de abusar o escalar privilegios, les permiten, a su vez, a tomar acciones indebidas que podría cambiar o detener otros servicios necesarios y esenciales para el correcto funcionamiento de la CS (p. ej. denegación de los heartbeats al CSMS), del proceso de carga de un EV (p. ej. interrumpir la carga de un conector del EVSE) o provocar serios apagones por impactar en el grid (p. ej. retornar energía en escenarios V2G). Aparte de esto, agentes maliciosos pueden acceder a datos sensibles y registros almacenados en la CS con la posibilidad de filtrarlos a un actor malicioso (p. ej. un gateway externo al sistema para exfiltración de los datos), o incluso, alterarlos para engañar al propio MAS o al sistema de pago de la red de carga. Es más, agentes legítimos pueden ser diseñados para efectuar tareas de monitorización con la capacidad para analizar el tráfico de red y las comunicaciones entre la CS y sus componentes relacionadas (ya sea otra CS o el CSMS). Si estos agentes son manipulados, entonces pueden tener también la capacidad para liderar acciones de escuchas indebidas.

3.2. Clase 2: agentes SW y el sistema de control (CSMS)

En la mayoría de escenarios, las CS pueden no ser los únicos nodos en los que se ejecutan agentes SW, sino que muchas veces es necesario situar la centralización de datos y comandos en otros agentes desplegados fuera de las estaciones. Un lugar idóneo para ello, es el CSMS puesto que este gobierna todas las CS de la red y tiene una visión global de todo el sistema. Los agentes presentes en el CSMS están diseñados para obtener datos de todos los demás agentes SW desplegados por la red, con el fin de elaborar estadísticos y mantener informado al CSMS. Por lo tanto, estos tipos de colectores necesitan mantener enlaces de comunicación con el sistema central.

Al tratarse el CSMS de un nodo de gestión centralizada, es una pieza clave dentro de la infraestructura de carga, por lo que los agentes integrados en él pueden ser manipulados por insiders maliciosos (ej. un CSO) quienes pueden tomar el control de toda la red de carga y lanzar numerosos tipos de ataques. Por ejemplo, la manipulación de datos falsos correspondientes a estados de salud hacia el CSMS, y la interrupción de operaciones de control hacia el CSMS/CS para violar la ejecución natural de otros servicios esenciales como la gestión de transacciones de energía o su control (p. ej. abusar de los canales de comunicación y aislar al CSMS o una CS, en esta última se podría sobrecargar al controlador y obligar a la estación a gestionar operaciones en modo offline como es indicado en [2] y [11]). Además, en el CSMS se almacenan datos y estadísticos relativos al consumo y al funcionamiento de toda la red EVSE, por lo un agente “rogue” integrado en el CSMS tendría acceso a tal información, con lo cual podría obtener una imagen detallada de toda la topología e información sensible de la red (a nivel de información y operación). Insiders también podrían inyectar malware o bombas lógicas (ej. backdoors) en los códigos de los agentes, otorgándoles la capaci-

dad para engañar a los CSO sobre el estado real de la red, consiguiendo que amenazas de tipo APT puedan surgir en estos contexto, en el que insiders/outsiders podrían navegar de manera sigilosa de un nodo a otro de la red de carga y de control (p. ej. de un agente SW malicioso a otro). Por otro lado, insiders y outsiders podrían suplantar la identidad del CSMS para gestionar instrucciones de C&C hacia los agentes SW de las estaciones a fin de causar DoS y, consecuentemente, fraude o robo de energía. Es decir, adversarios con el control total de un agente SW en una estación podría causar exhaustación para interrumpir servicios de comunicación y aislar la estación como es señalado arriba. De este modo, la estación podría entrar en modo offline por requisitos del protocolo OCPP [2] (ver sección 2), obligándola a tratar las autorizaciones (probablemente ilícitas) en local a fin de garantizar el servicio y la continuidad de negocio. Pero también, entidades supuestamente lícitas falseando la identidad de colectores o el CSMS podrían recibir información del sistema para liderar ataques contra la confidencialidad. Esta última amenaza puede ocurrir si medidas de seguridad en canales de comunicación (p. ej., usando TLS) no son consideradas. Incluso, siendo consideradas y dependiendo de las medidas de seguridad, es posible conllevar ataques MiTM, corrompiendo los canales de comunicación tal como se detalla en [13] para TLS 1.3 y en [11] para OCPP sobre TLS.

3.3. Clase 3: agentes SW y otros agentes SW

La propia definición de los MAS menciona que un agente tiene la capacidad de interaccionar con otros agentes en la búsqueda de realizar las tareas para las que fue diseñado. En el caso de las infraestructuras de carga, estas interacciones se refieren a las comunicaciones que se dan entre los agentes de distintas estaciones para intercambiar información sobre el estado de la red y el consumo de energía que los usuarios están demandando. También en esta categoría se distinguen las comunicaciones entre los agentes de las CS y los agentes (los colectores) que se encuentran en el CSMS, tanto para el proceso de recolección de información por áreas, como para el envío de comandos por parte de CSO a las estaciones. Si alguno de los agentes involucrados en estas interacciones ha sido comprometido por un insider/outsider, podría usarse para engañar al sistema MAS en su totalidad y extender la zona de influencia del atacante y su superficie de ataque.

Un agente comprometido podría hacerse pasar por otro agente SW con el fin de engañar y entorpecer el funcionamiento del sistema de monitorización MAS. Además, también podría mentir sobre su rol, suplantando a un agente recolector, haciendo que todos los agentes de la red le envíen su información al agente equivocado. Un agente malicioso también puede negarse a responder a las peticiones de otros agentes que intenten comunicarse con él, o incluso, realizar otros tipos de ataques de DoS, como, por ejemplo: flooding (provocar el colapso de una red por el envío masivo de paquetes), selective forwarding (retransmitir de manera selectiva) o crear agujeros negros (black holes) propiamente dicho, muchos de los cuales definidos en [11] y [14]. Otro problema que puede surgir de la interacción entre dos agentes es el caso en el que el agente malicioso niegue haber realizado una acción, como puede ser el de enviar cierta información a otro agente. Esto puede provocar dificultades a la hora de realizar auditorías del sistema que intenten descubrir cómo se ha producido un incidente de seguridad.

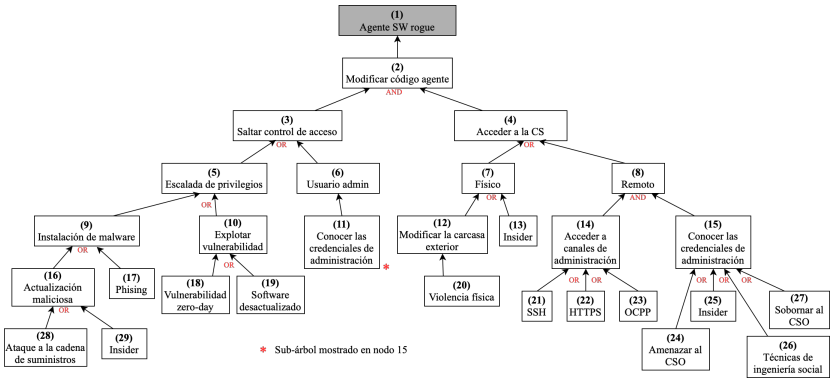

Figura 2: AT para obtener el control de un agente SW

Asociando todos estos ataques al modelo tradicional CIA y priorizando los riesgos dentro del contexto de energía y control, observamos que el hecho de que agentes maliciosos integrados cerca de los componentes principales de telemetría y control, pueden conllevar a serios ataques contra la disponibilidad e integridad de operaciones y servicios esenciales. Sin embargo, esto no quita la relevancia que tienen los ataques contra la confidencialidad.

4. Modelado de ataques contra agentes SW

Para estudiar la viabilidad de la arquitectura propuesta en la sección 2, basada en un MAS para infraestructuras de carga, se explora en esta sección algunas de las amenazas ya mencionadas en la sección anterior, a fin de identificar posibles vulnerabilidades dentro de nuestro sistema. En la literatura encontramos una gran cantidad de metodologías usadas para el modelado de ataques, como el modelo STRIDE [15], basado en el análisis de amenazas por componentes, la metodología STPA-sec [16], que estudia acciones que pueden llevar al sistema a un estado no seguro, o el enfoque OCTAVE, basado en el riesgo operacional y prácticas seguras [17]. Sin embargo, una de las más populares debido a su versatilidad son los árboles de ataque (Attack Tree, AT) [18] [19] [20] [21].

Los AT son un tipo de grafos lógicos que modelan secuencias de múltiples posibles acciones llevadas a cabo por actores maliciosos para evadir un sistema de defensa y realizar un ataque. Estos árboles se confeccionan en base a tres componentes gráficos principales [20]: nodos, aristas y puertas lógicas. Entre los nodos, destacan: el nodo raíz, que representa el objetivo del ataque; los nodos internos, por su parte, se corresponden con objetivos parciales; mientras que los nodos hoja, son los ataques que consideramos atómicos (es decir, que no pueden descomponerse más, o simplemente aquellos que no interesa especificar más detalles). Las puertas lógicas pueden ser conjuntivas, lo que implica que todos los requisitos deben cumplirse, o disyuntivas, o que supone que cualquiera de los requisitos es suficiente para llegar al nivel inmediatamente superior. Entre las fortalezas de los AT encontramos el hecho de que se pueden

representar el formato texto, lo que posibilita la traducción a otros lenguajes y formas de representación de los datos como XML [19] o JSON [22]. Por tanto, son fáciles de automatizar y de integrar con otros sistemas de información [23]. Además, los árboles pueden almacenarse en un repositorio y reusarse para generar nuevos árboles que extiendan los ya existentes. Como contrapartida, nos encontramos con que su construcción se basa en el conocimiento y la experiencia del analista que los confecciona, por lo que es fácil omitir posibles ataques y rutas. Otra debilidad es que no existe un estándar para su creación, simulación y análisis [21].

Una vez explicado la técnica, vamos a analizar mediante AT, algunos de los objetivos que pueden tener insiders u outsiders en el contexto de infraestructuras de cargas controladas por un MAS. Como no es viable presentar un estudio exhaustivo de todos los posibles objetivos de un atacante por restricciones de espacio, en este análisis sólo se tendrán en cuenta algunos de los ataques que afecten a la integridad y a la disponibilidad, que, por su parte, son los tipos de ataques que más nos interesan, ya que pueden: ocasionar daños en la infraestructura y su monitorización, impedir a los usuarios que puedan cargar sus VE o proceder con fraudes relevantes en el consumo abusivo de energía.

Concretamente, se ha considerado una **ataque contra la integridad**, donde el objetivo es ganar el control de un agente SW integrado dentro de una CS correspondiente a la primera categoría definida en la sección anterior (ver subsección 3.1), modificando su comportamiento (convirtiéndolo en un agente "rogue") para comprometer la CS. Esto lo capacita para llevar a cabo ataques más complejos, que le pueden suponer mayores beneficios y ocasionar un mayor impacto en la infraestructura. En la figura 2 se presenta el árbol de ataque que desglosa las rutas a seguir por un adversario para comprometer un agente SW en el MAS ($1 -$ ilustra el nodo en la figura) propuesto en este artículo. Todos los vectores de ataque considerados en este punto pasan por alterar el código fuente que implementa el agente SW (2), para lo cual, es necesario: (i) acceder de alguna forma a la CS (4) y (ii) escalar privilegios para alcanzar dicho código (3). Es importante resaltar que el acceso a la CS puede ser tanto físico (7), como remoto (8). Si tenemos en cuenta los casos en los que un atacante (insider u outsider) se presenta en los dominios físicos de la estación de carga, podemos diferenciar dos casos. El primero de ellos es que el atacante acceda a los puertos físicos de la CS, pensados para las tareas de administración, y mediante la manipulación física de la carcasa externa del cargador (12). Esto lo conseguiría directamente ejerciendo violencia física contra el sistema (20). Sin embargo, también hay que contemplar la posibilidad de que el atacante sea un operario o técnico de mantenimiento (13).

No es necesario que el atacante se encuentre en el mismo lugar que la CS para perpetrar un ataque. El controlador de la CS está conectado a la red y expone servicios a través de diferentes protocolos para acceder a él de forma telemática y llevar a cabo tareas de administración y mantenimiento. En este caso, un atacante puede usar estos canales para alcanzar la CS, pero para ello antes deberá ser capaz de infiltrarse en la red en la que se encuentra el cargador y localizar la dirección y los puertos en los que se están ejecutando dichos servicios (14). Los protocolos más comunes para este cometido son SSH, HTTPS y OCPP sobre TLS (como indicado en la figura como 21, 22 y 23, respectivamente) que por defecto están protegidos por mecanismos de seguridad (p. ej., la autenticación se puede establecer con usuario y contraseña, criptografía de clave

pública o certificados). Por tanto, su uso está vinculado a personal autorizado, por lo que otra tarea que deberá liderar un atacante será la de robar las credenciales de acceso (15), ya sea mediante técnicas de ingeniería social (26), amenazando (24) o sobornando (27) a algún operario del sistema, es decir, a un CSO. También está la posibilidad de que el atacante sea el propio operario o el administrador del sistema (p. ej. un trabajador descontento) (25).

Una vez el atacante ha alcanzado la CS objetivo, deberá eludir el control de acceso para llegar al código fuente del agente SW (3), con el fin de comprometerlo. Esto puede llegar a ser sencillo si el atacante conoce las credenciales (7) de una cuenta con los privilegios de administración (6), que ha podido conseguir de múltiples formas (24, 25, 26, 27), como se menciona en el párrafo anterior. En cambio, si el atacante usa una cuenta sin los privilegios para modificar el código del agente, deberá valerse de otras técnicas para realizar una escalada de privilegios (5). Una de ellas podría ser la de aprovecharse de alguna vulnerabilidad del sistema (10) que aún no haya sido parcheada, ya sea porque el personal de administración no ha realizado bien su trabajo (19), o porque se trate de una vulnerabilidad desconocida, zero-days (cero día), (18). Otra forma de escalar privilegios sería mediante la instalación de un malware (9), la cual puede ejecutar una puerta trasera para permitir el control desde una localización remota. Para infectar la CS, el atacante cuenta con múltiples opciones, como las campañas de phishing o spear phishing (17). También, es importante contemplar la opción en la que el atacante comprometa el sistema de actualizaciones (28), de forma que la CS lleve a cabo una actualización maliciosa (16) e instale el malware sin que el administrador se percate. Una vez más, aparece la opción del insider, ya que puede autorizar actualizaciones no oficiales (29).

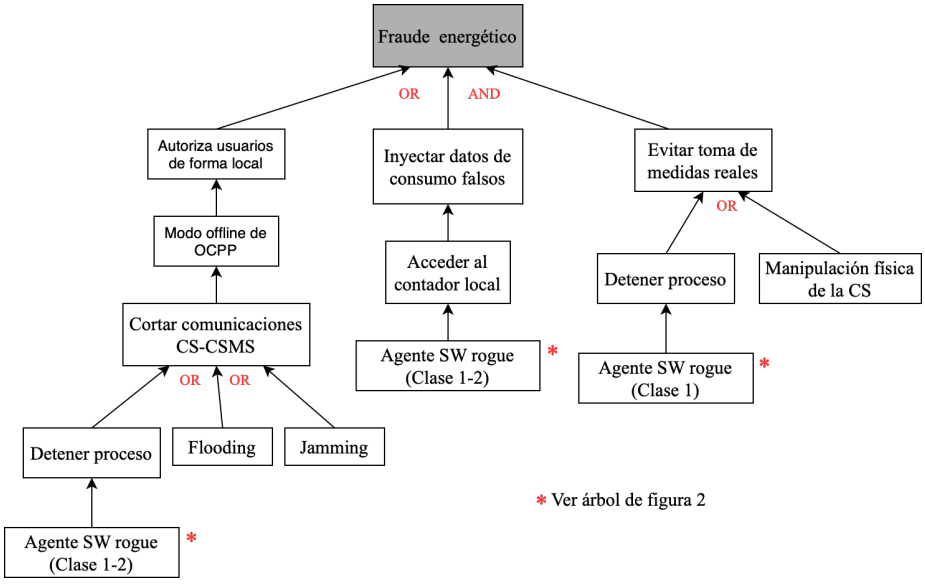

Figura 3: AT para cometer fraude energético

Una vez que el atacante se ha hecho con el control del agente, éste es capaz de plantearse ataques más sofisticados que pueden incluso ser de tipo APT para persistir aún más en el tiempo. Esto supone que el árbol descrito en la figura 2 se convierte en un componente de muchos otros árboles de ataque que representan diversos objetivos, como se puede apreciar en la figura 3. Aquí se muestra una de las características que se han comentado anteriormente y que hacen a los AT ser una herramienta muy versátil en el análisis de amenazas: *su capacidad para reutilizarse y componer árboles más complejos*. En la figura 3 se observa un árbol para un **ataque de fraude de energía** que sirve de ejemplo para ilustrar este hecho. En él, el nodo raíz del árbol de la figura 2 se ha convertido en un nodo hoja, esto significa que el objetivo final que considerábamos anteriormente se convierte en el punto de partida para un nuevo objetivo del atacante.

En la figura 4 se presenta un ejemplo de **ataque de denegación de servicio** en el que el objetivo del atacante es impedir las comunicaciones entre dos agentes SW. Por motivos de extensión del documento no va a explicarse detalladamente todo el árbol, aunque sí es interesante pararse en algunas partes del mismo. Este árbol está estructurado de forma que diferencia entre vectores de ataque provenientes de la capa física (4), los del nivel de red (2) y los del nivel de aplicación (5). Si atendemos a los ataques de red (2), vemos que la mayoría de ellos (black-hole attack (5), flooding (6) y selective forwarding (7)) requieren antes de un ataque de suplantación de identidad (13). De esta forma un atacante necesita llevar a cabo un ataque de ARP spoofing (19) y, a través de un agente rogue modificado (20), afirmar ser otro agente legítimo de la red para engaña a los agentes de otras estaciones (y también al agente recolector del CSMS). La excepción que no necesitaría una suplantación de identidad previa, es el ataque de replay (8), en el que el atacante, únicamente captura un paquete de una conversación antigua y lo envía múltiples veces al objetivo que desea dejar fuera de servicio en un corto período de tiempo.

A nivel de aplicación (3) se pueden detener las comunicaciones entre dos agentes, lanzando una señal de terminación (9) al proceso encargado de escuchar en el puerto correspondiente. Esto lo puede realizar de forma automática un malware previamente instalado en el nodo (14) o, nuevamente, un agente SW cuyo comportamiento ha sido modificado (16). Un atacante también tendría la opción de infiltrarse en la CS y obtener una terminal remota (15), conectándose a través de protocolos como SSH (26) o Telnet (27). Además, de ello también necesitará tener los permisos suficientes como para detener procesos del sistema (22), que pueden obtenerse mediante una escalada de privilegios (24), o usando las credenciales de un CSO (25).

5. Recomendaciones de seguridad

Para garantizar la seguridad de un MAS desplegado en una infraestructura de carga de VE, deben cumplirse una serie de requisitos de seguridad para reducir cualquier incremento de riesgo que vaya en contra del buen funcionamiento y rendimiento de los posibles agentes SW desplegados en las CS, en el CSMS y entre CS. Uno de los requisitos de seguridad a abordar durante el diseño de un MAS y en relación con el CIA, es la importancia que tiene el intercambio fluido de datos (ya sea con otros agentes o con la plataforma en la que se hospedan), vital para garantizar una monitorización fiable

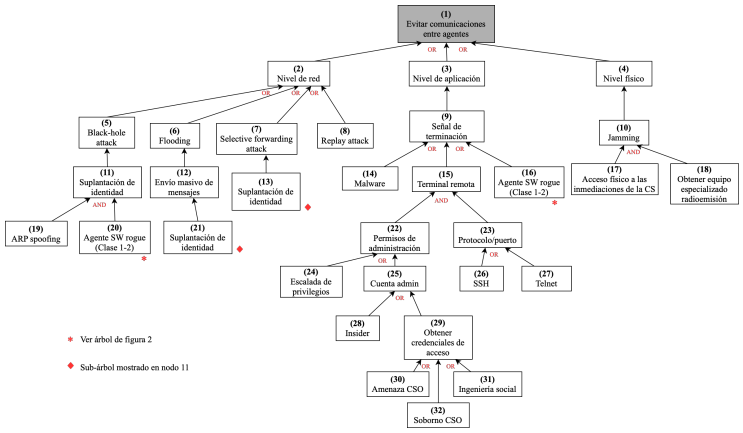

Figura 4: AT para impedir que dos agentes se comuniquen

de la infraestructura de carga. Esto implica configurar y usar protocolos y mecanismos de seguridad bajo algoritmos de cifrado robustos, uso de certificados digitales como medio de autenticación, firmas digitales para autenticación y prueba de las acciones cometidas en cada una de las transacciones, así como medidas de validación mediante hashes. Sin embargo, esto puede acarrear penalizaciones en la eficiencia de la CS, ya que en la mayoría de ocasiones, se tratan de dispositivos con importantes limitaciones de recursos HW y SW, con poca capacidad de cómputo (p. ej., sistemas empotrados).

Por otro lado, los agentes SW pueden estar expuestos a actores maliciosos internos o externos, ya que las CS pueden estar desplegadas en dominios públicos. Como ya hemos analizado en la sección 4, estos actores pueden tener la habilidad para modificar los códigos fuentes de los agentes y su comportamiento, capacitándoles a realizar subsecuentes ataques que puede conllevar a un impacto mayor en la red EVSE y la disponibilidad de los servicios esenciales (la energía). Por tanto, se recomienda que aunque los agentes no puedan evitar la modificación de su propio código, es necesario que la CS intensifique las medidas de control acceso al sistema para proteger el acceso directo al código de los agentes SW, registrando cada acción cometida dentro de la misma para dar garantías de auditoría y responsabilidad (*accountability*), por lo que también se recomienda combinar las medidas de protección con el uso de tecnologías disruptivas como es la tecnología de blockchain para la trazabilidad [3]. Además de esto, también es aconsejable proteger frente a accesos no autorizados los archivos de registro y la información con la que operan los agentes.

Las amenazas que afectan a la disponibilidad de los agentes SW suelen ser difíciles de contrarrestar. Por lo general, un agente SW debe ser capaz de procesar y responder a las peticiones de otros agentes SW de la forma más eficiente posible, sin llevar a cabo cómputos muy costosos en recursos, de forma que pueda hacer frente al mayor número posible de peticiones en un período de tiempo. Por otro lado, esto se contradice con el resto de requisitos de seguridad que suelen consistir en comprobaciones en las que se realizan cálculos, por lo general, complejos. Por tanto, es conveniente que el sistema MAS integre otras herramientas de detección y monitorización de red que asistan a

detectar y mitigar posibles amenazas, especialmente contra la DoS cuando se observen comportamientos de tráfico de red sospechosos, tales como IDS, IPS, SIEM, firewalls, etc. Evidentemente, estas soluciones deben estar bajo políticas de seguridad siguiendo marcos políticos y legales, en el que se deben cumplir las normativas existentes (p. ej., el Real Decreto 43/2021 [24]), especialmente cuando existes irregularidades que pueden afectar a otras organizaciones relacionadas. Por ello, es fundamental activar las medidas de inteligencia, y establecer contacto con los equipos de respuesta ante incidencias, como pueden ser el INCIBE-CERT [25] o el CCN-CERT [26].

Como ya se comentado, cada acción que realice un agente SW dentro del sistema y para cada evento que detecte, deberá quedar registrado de forma que se identifique inequívocamente el autor de esa entrada del registro. Esto puede lograrse mediante técnicas de firma digital y funciones hash. El objetivo es evitar que un agente bajo el control del atacante pueda negar haber realizado una acción (p. ej. enviar cierta información a otro agente SW). Es más, al tratarse de un sistema distribuido y colaborativo, nuestro sistema MAS dispondrá de más de un archivo de registro, por lo que un mismo evento puede quedar registrado por dos agentes distintos. Esto mejora la protección frente a ataques de rechazo.

6. Conclusiones y trabajo futuro

Este trabajo ha recopilado un análisis extendido sobre las posibles amenazas en sistemas multi-agente, desplegados en infraestructuras de carga de vehículos eléctricos teniendo presente la arquitectura estandarizada de OCPP. La infraestructura incluye no solo la comunicación específica de OCPP para el control y la administración de energía, sino que, además, incluye una red de información paralela basada en agentes SW para contribuir y precisar en las tareas de monitorización, mantenimiento y seguridad. A través de la interacción con los respectivos agentes, se busca la forma de maximizar la consciencia situacional y la protección proactiva mediante la retroalimentación de otros sistemas esenciales de seguridad, como IDS/IPS, SIEM o SOC. Sin embargo, en este escenario de aplicación es también de vital importancia analizar previamente las amenazas que pueden traer esta tecnología al contexto mencionado, priorizando aquellas que pueden impactar principalmente en la gestión y distribución de energía a los usuarios finales. Es por ello, que este artículo científico incluye una agrupación de agentes de acuerdo a los principales elementos de control según el protocolo OCPP y en base a las funciones e interacciones que pueden tener los agentes dentro de dicho escenario. En base a esta agrupación, se ha identificado diversos ataques siguiendo las recomendaciones dadas por el SP 800-19 definido por el NIST, y se ha modelado formalmente dichas amenazas en base a la metodología tradicional de árboles de ataques.

Concluimos que es fundamental considerar la influencia positiva del uso de agentes, pero priorizando los riesgos que puede conllevar su uso, ofreciendo a la comunidad científica y a la industria una base por la cual entender dichos riesgos e identificar posibles medidas de protección, también proporcionadas en este artículo. En el futuro, pretendemos, por un lado, integrar el MAS dentro de una infraestructura de carga real y dentro del proyecto “Smart and Secure EV Urban Lab II”, y, por otro lado, automatizar la metodología para que los árboles de ataques puedan ser integrados como parte de la

monitorización de esta infraestructura, extrayendo métricas y modos de evaluación.

Agradecimientos

Trabajo financiado por el proyecto "Smart and Secure EV Urban Lab II", perteneciente al II Plan Propio Smart Campus de la Universidad de Málaga, y por el proyecto SAVE (P18-TP-3724), perteneciente a la Junta de Andalucía.

Referencias

[1] Meticulous Research, "Electric Vehicle Market Worth $2,495.4 Billion and 233.9 Millions Units by 2027," https://www.meticulousresearch.com, 2021.

[2] Open Charge Alliance. Open Charge Point Prorocol (OCPP) 2.0.1. https://www.openchargealliance.org/protocols/ocpp-201/.

[3] H. ElHusseini, C. Assi, B. Moussa, R. Attallah, and A. Ghrayeb, "Blockchain, AI and Smart Grids: The three musketeers to a decentralized EV charging infrastructure," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 24–29, 2020.

[4] M. Pagani, W. Korosec, N. Chokani, and R. S. Abhari, "User behaviour and electric vehicle charging infrastructure: An agent-based model assessment," *Applied Energy*, vol. 254, p. 113680, 2019.

[5] J. Miranda, J. Borges, D. Valério, and M. J. Mendes, "Multi-agent management system for electric vehicle charging," *International Transactions on Electrical Energy Systems*, vol. 25, no. 5, pp. 770–788, 2015.

[6] C. B. Saner, A. Trivedi, and D. Srinivasan, "A Cooperative Hierarchical Multi-Agent System for EV Charging Scheduling in Presence of Multiple Charging Stations," *IEEE Transactions on Smart Grid*, 2022.

[7] K. Chaudhari, N. K. Kandasamy, A. Krishnan, A. Ukil, and H. B. Gooi, "Agent-based aggregated behavior modeling for electric vehicle charging load," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 856–868, 2018.

[8] E. Y. ElBanhawy, R. Dalton, E. M. Thompson, and R. Kotter, "A heuristic approach for investigating the integration of electric mobility charging infrastructure in metropolitan areas: An agent-based modeling simulation," in *2012 2nd International Symposium On Environment Friendly Energies And Applications*. IEEE, 2012, pp. 74–86.

[9] W. Jansen and T. Karygiannis, "Mobile agent security, SP 800-19," National Institute of Standards and Tecnology, Tech. Rep., 1998.

[10] AMPECO, "Enable innovation and cost efficiency with OCPP," https://www.ampeco.com, 2022.

[11] C. Alcaraz, J. Lopez, and S. Wolthunsen, "OCPP Protocol: Security Threats and Challenges," *IEEE Transactions on Smart Grid*, vol. 8, pp. 2452 – 2459, 02/2017 2017.

[12] J. E. Rubio, C. Alcaraz, and J. Lopez, "Addressing Security in OCPP: Protection Against Man-in-the-Middle Attacks," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018, pp. 1–5.

[13] T. Jager, J. Schwenk, and J. Somorovsky, "On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS1 v1.5 Encryption," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 1185–1196. [Online]. Available: https://doi.org/10.1145/2810103.2813657

[14] T. Tsar, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL)," Routing Over Low-Power and Lossy Networks, IETF, Tech. Rep., 2014.

[15] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," in *2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*. IEEE, 2017, pp. 1–6.

[16] W. Young and N. G. Leveson, "An integrated approach to safety and security based on systems theory," *Communications of the ACM*, vol. 57, no. 2, pp. 31–35, 2014.

[17] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the OCTAVE Approach," Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, Tech. Rep., 2003.

[18] S. Haque, M. Keffeler, and T. Atkison, "An evolutionary approach of attack graphs and attack trees: A survey of attack modeling," in *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer, 2017, pp. 224–229.

[19] D. Vitkus, J. Salter, N. Goranin, and D. Čeponis, "Method for Attack Tree Data Transformation and Import Into IT Risk Analysis Expert Systems," *Applied Sciences*, vol. 10, no. 23, p. 8423, 2020.

[20] S. Pasandideh, L. Gomes, and P. Maló, "Improving attack trees analysis using Petri net modeling of cyber-attacks," in *28th International Symposium on Industrial Electronics (ISIE)*. IEEE, 2019, pp. 1644–1649.

[21] G. Dalton, R. F. Mills, J. M. Colombi, R. A. Raines *et al.*, "Analyzing attack trees using generalized stochastic petri nets," in *Information Assurance Workshop*. IEEE, 2006, pp. 116–123.

[22] D. Beaulaton, N. B. Said, I. Cristescu, and S. Sadou, "Security analysis of IoT systems using attack trees," in *International Workshop on Graphical Models for Security*. Springer, 2019, pp. 68–94.

[23] D. Kim, Y.-H. Kim, D. Shin, and D. Shin, "Fast attack detection system using log analysis and attack tree generation," *Cluster Computing*, vol. 22, no. 1, pp. 1827–1835, 2019.

[24] Agencia Estatal Boletín Oficial del Estado, "Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información," https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-1192, 2018.

[25] Instituto Nacional de Ciberseguridad de España, "INCIBE-CERT," https://www.incibe-cert.es, 2022.

[26] Centro Criptológico Nacional, "CCN-CERT," https://www.ccn-cert.cni.es, 2022.