Aspectos de seguridad en un sistema de IOT para controlar la calidad del aire

Paula Venosa[1], Sofía Martin[1], Patricio Bolino[1], Paula Durán[1], Lautaro Canales[1]
[1] LINTI - Facultad de Informática - Universidad Nacional de La Plata
pvenosa@info.unlp.edu.ar, smartin@linti.unlp.edu.ar, patriciobolino@gmail.com, paumduran@hotmail.com, lautarocanales@gmail.com

Abstract. La Internet de las cosas (IoT) ha crecido y ampliado su uso a lo largo de los últimos años, aplicándose en ámbitos de la industria, ahorro de energía, mejoras de servicios gubernamentales, entre otros. Por lo que su seguridad ha generado mayor interés debido a los datos que se adquieren, transmiten y procesan. En este artículo se evalúan aspectos de seguridad a tener en cuenta concentrándose en un caso particular de implementación y se proponen posibles mitigaciones para mejorar las debilidades de seguridad existentes.

Keywords: Seguridad IoT; Automatización CO2; Seguridad;.

1 Introducción

Actualmente el uso de tecnologías que permiten automatizar funciones avanza cada día más, permitiendo transformar las ciudades en "inteligentes" con el fin de mejorar sus servicios y la calidad de vida de sus ciudadanos [1], [2]. Esta transformación liderada por los dispositivos IoT (Internet of Things o Industrial Internet of Things) está ayudando tanto a las grandes metrópolis, como a las pequeñas ciudades a mejorar los servicios que prestan y a permitir la comunicación de la información. Su expansión ha permitido pensar en aspectos que permitan prácticas de ahorro de energía inteligentes, infraestructuras con servicios automatizados para simplificar la vida en los hogares, y el paradigma de una industria 4.0 [3].

Algunos de los aspectos a tener en cuenta cuando se trabaja con dispositivos IoT, es profundizar no solamente en las necesidades técnicas que se espera cubrir con los mismos sino también poner especial atención al nivel de protección ante ataques que puedan afectar a la privacidad de los datos, de la organización y de los usuarios, o impedir el correcto funcionamiento de su actividad [4].

Las organizaciones que conectan a sus redes dispositivos IoT deben tener en consideración la importancia de garantizar la seguridad, a través del fortalecimiento de la red donde se conectan los dispositivos [5], del análisis y configuración de los dispositivos, del monitoreo del tráfico y actividad de los mismos así como de contar con un plan para gestionar los incidentes en dicho marco [6].

El análisis de vulnerabilidades es un paso importante a la hora de construir arquitecturas que transmiten datos por red y en particular aquellas que utilizan dispositivos IoT ya que permite identificar debilidades y mitigar así posibles

amenazas, para mejorar el nivel de seguridad de los sistemas. El paso más importante para evaluar las mejoras para securizar un sistema es en la etapa de diseño, gestionando luego un proceso contínuo de mejoras cuando el sistema ya ha sido implementado.

Es por ello que desde el LINTI, en el marco de la línea de investigación de seguridad en IOT, se trabaja desde el año 2017 en el análisis y mitigación de vulnerabilidades en diferentes proyectos: “Análisis y mejoras de seguridad a una aplicación prototipo en IoT” [7], “Hackeamos para construir robots seguros” [8] e “Identificación de vulnerabilidades en ambientes IOT” [9]. En el marco de este último se realizó el trabajo que se presenta en este artículo.

2 Ciberseguridad y aplicaciones IoT

En la actualidad la seguridad en sistemas informáticos ha cobrado cada vez mayor importancia debido al crecimiento en su uso que hace que las organizaciones basen sus principales funciones en dichos sistemas. Una de las áreas involucradas son aquellos sistemas que incluyen dispositivos IoT, la cual ha cobrado mucha relevancia debido a la masividad de su uso [10] y a la importancia de proteger los datos confidenciales que estos procesan. A su vez, deben implementarse controles en la seguridad física ya que este tipo de dispositivos se encuentran dispuestos por fuera de los centros de datos y suelen quedar excluidos del “radar” de los equipos de seguridad informática, comunicaciones e infraestructuras.

La creciente disponibilidad de los mismos ha permitido su implementación con diversos fines, dado que en general son placas que cuentan con varios puertos de conexión, con capacidad de gestionar funcionalidades simples en función de los valores recibidos. Estos puertos permiten conectar diferentes tipos de sensores, actuadores, dispositivos RFID, entre otros y en general el procesamiento local es mínimo, debido a la capacidad del procesador [2]. Esta característica propia de los dispositivos IoT genera que en muchos casos la información se envíe a servidores remotos que centralizan los datos de uno o más dispositivos.

Una de las aplicaciones de los dispositivos IoT, como mencionamos anteriormente, es permitir sensar información del ambiente para, no solo poder reportar los datos, sino también generar alguna acción concreta que dé cuenta de un cambio ocurrido. Este tipo de desarrollos permite automatizar el control de temperaturas, movimiento en un ambiente delimitado, entre otras cosas.

La información enviada, en muchos casos, es a través de la tecnología Wi-Fi, es por ello que la seguridad de los datos se torna crítica y en función de la capacidad del procesador entran en juego las limitaciones para implementar protocolos de encriptación u otras medidas para incrementar la seguridad.

Diferentes organizaciones referentes en controles de ciberseguridad para tecnologías IT comenzaron a desarrollar estándares y frameworks dentro de sus programas de buenas prácticas enfocados a los dispositivos y las aplicaciones IOT. Entre ellos podemos nombrar a la iniciativa OWAP [11] con su Top Ten de vulnerabilidades comunes en IOT, NIST (National Institute of Standards and

Technology) [12] con su programa de ciberseguridad para IOT que incluye estándares, guías y herramientas y colabora con fabricantes, gobiernos, consumidores y universidades, CIS (Center for Internet Security) [13] con el desarrollo de una guía de controles que recorre diversos aspectos tales como la protección de los datos, la gestión en el control de los accesos, las configuraciones de seguridad, las protecciones para el correo electrónico y los navegadores web, el monitoreo de las redes, las defensas ante malware, y la IoTSF que se autodefine como un "super Blue Team[1]" de usuarios, profesionales de seguridad, proveedores de productos de hardware y software de IoT, operadores de red, y otros actores del mundo del IoT, que tienen como misión colaborar en mejorar la seguridad de las aplicaciones de IoT, a través de grupos de trabajo, documentación y distintas herramientas que proveen en el marco de su comunidad [14], entre otros.

Existen diferentes propuestas de metodologías para implementar planes de control de amenazas que pueden afectar a un escenario, para lo cual es necesario evaluar procesos, el hardware del dispositivo, el software, las interfaces cableadas e inalámbricas, la autenticación y la seguridad en la capa de aplicación [6]. Cabe destacar que, si bien la mayoría de los escenarios comparten similitudes, la implementación de cada uno debe evaluarse en función del servicio que presta.

Las organizaciones mencionadas anteriormente dan cuenta de que hoy día ya existen herramientas para evaluar la seguridad de los dispositivos IoT, por lo que es necesario al momento del desarrollo de software y hardware IoT minimizar las amenazas y vulnerabilidades más comunes. Estas precauciones permiten evitar incidentes de seguridad que se traduzcan en la pérdida de confianza hacia estas nuevas tecnologías.

En este contexto se propone un análisis de un caso de uso aplicable a diferentes ámbitos de trabajo, que implementa esta tecnología y los diferentes aspectos evaluados para definir mejoras tanto a nivel del software como a nivel físico.

3 Ciberseguridad y aplicaciones IoT

Debido a la importancia que ha cobrado estos últimos años el control de la calidad del aire en ambientes cerrados o pocos ventilados, han surgido desarrollos que automatizan el control de estos valores permitiendo establecer un ambiente seguro de trabajo. Este servicio fue pensado construyendo un sistema con un dispositivo IoT junto con un sensor de dióxido de carbono en cuanto al hardware y un desarrollo de software que acompañe la visualización y registro histórico de los datos.

El escenario que detallaremos se compone de un dispositivo IoT que realiza mediciones del entorno, una red que tiene conexión a Internet y diferentes dispositivos (computadoras y equipos móviles) que interactúan para permitir la visualización de los datos del dispositivo a través de un portal web.

[1] Blue Team: grupo de especialistas en seguridad que rastrean ciber incidentes y realizan análisis de los sistemas para garantizar la seguridad, identificar posibles fallos y verificar la efectividad de cada medida.

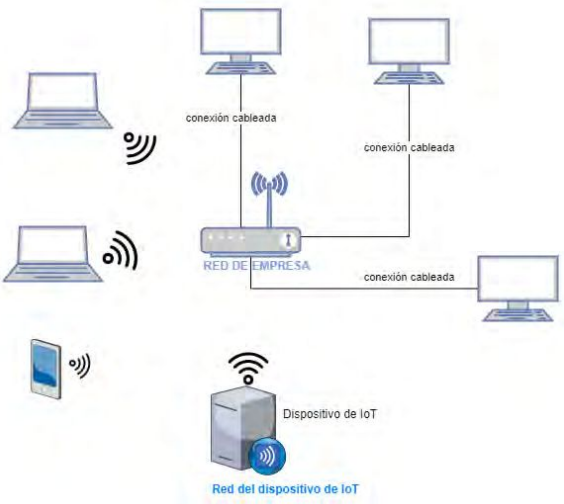

Fig 1. Arquitectura del escenario

3.1 Arquitectura del prototipo

El prototipo que permite sensar datos del ambiente e informarlos, como así también generar una alarma en función de la configuración inicial está compuesto por:

- Una placa NodeMCU[15].
- Un sensor CO2.
- Un servidor web.

En forma general, el rol de la placa es sensar los datos de ambiente y, en función de un programa interno, generar una alarma cuando los valores no son los normales. Además todos los datos censados son enviados por medio de una conexión wireless a un servidor web..

La placa NodeMCU es muy utilizada en dispositivos IoT por su tamaño, facilidades de uso y bajo costo. Una de las ventajas de esta placa es que tiene incorporado el microchip ESP8266 System-on-Chip (SoC) que simplifica la conexión y el procesamiento local de la comunicación. El microchip ESP8266 es un microcontrolador capaz de ejecutar código de forma local en varios lenguajes de programación y habilita la conexión a redes inalámbricas desde el programa que se grabe. Este es un módulo Wi-Fi pequeño, utilizado para establecer una conexión entre un microcontrolador o procesador y una red inalámbrica. El mismo puede trabajar tanto como un sistema independiente como conectado a otras redes inalámbricas disponibles. Se entiende un sistema independiente a la capacidad de disponer de una red inalámbrica propia a la cual se pueden conectar dispositivos.

En el caso particular de este proyecto se utilizan ambos modos disponibles para diferentes propósitos:

- Levantar una red propia (con su propio SSID) que permite generar las configuraciones iniciales necesarias que detallaremos más adelante.

- Para conectarse a una red externa que permite acceder a Internet y mandar los datos al registro externo o servidor web.

Al momento de evaluar las placas disponibles para el sistema, el hecho de que el firmware y las herramientas de desarrollo sean open source es importante para el desarrollo y adaptación a los proyectos propios. Otras de las características relevantes es la interfaz USB a UART, la cual permite comunicarse mediante USB con el SoC. Posee a su vez un circuito capaz de regular tensiones de entrada desde 4.8V hasta 12V, a un valor de operación de 3.3V. Por último, se puede mencionar que cuenta con pulsadores que permiten reiniciar o borrar la memoria del módulo en casos de fallas del sistema.

Otra de las partes del prototipo es el sensor de CO2 que permite detectar los valores del ambiente, también tiene la capacidad de ser calibrado para establecer los valores normales de referencia. Y, por último, el servidor web cuenta con un portal que permite acceder a los datos provistos por el sensor, como así también tiene la posibilidad de guardar un histórico de los niveles captados en un registro externo. El acceso a los datos es a través de un usuario y clave para seguridad del acceso.

3.2 Funcionamiento general del sistema

Los dispositivos que se utilizan para generar alguna alarma en función de los valores medidos del entorno requieren que se indique cuáles son los valores que son normales al momento de sensar. Por lo cual una de las primeras acciones necesarias es realizar una calibración antes de su utilización ya que, a través de luces externas se indican los posibles estados según los valores tomados en las mediciones. Dicho dispostivo posee tres luces para indicar el estado del ambiente, verde (aún está ventilado), amarillo (es una alerta de que pasó los niveles bajos) y rojo (el ambiente no está correctamente ventilado, puede ser el aire estancado o viciado que aumenta el riesgo de contagios en caso de COVID).

En el caso que los valores censados por el dispositivo sobrepasen el umbral establecido, es decir que los niveles de toxicidad del entorno pueden llegar a generar complicaciones para la salud de las personas, se encenderá una alarma sonora. Esta alarma tiene la capacidad de poder desactivarse en forma manual para evitar ruido constante por medio de un botón. En el caso que se mantenga apretado una cantidad de segundos determinada, habilita la configuración para calibrar el sensor de CO2.

El puerto USB de la placa es utilizado para la programación del mismo, a través del cual se graba el software que realizará el control de los valores del ambiente y enviará la información al servidor web. Además de permitir la carga del programa provee la posibilidad de cargar el dispositivo eléctricamente.

Hay dos formas de realizar la conexión con el sistema de medición de CO2 para obtener los datos de las mediciones. En la primera de ellas, el dispositivo IoT puede conectarse a la red como un host más para habilitar el acceso a la información recolectada a través de un servicio web. Si la red tiene Internet, es posible configurar un servidor para que el dispositivo le envíe la información de las mediciones. En la segunda opción, el dispositivo IoT puede abrir su propia red Wi-Fi para publicar los

datos de las mediciones sin necesidad de que el usuario ni el dispositivo tengan que estar conectados a una red externa. De este modo, la nueva red Wi-Fi con nombre RedA aloja el sitio web a través de la IP privada del dispositivo para que el usuario pueda visualizar los datos de las mediciones.

Para poder configurar el dispositivo, se puede abrir una nueva red Wi-Fi, denominada Config_RedA que permite al usuario modificar la red Wi-Fi a la que se conecta el dispositivo para disponibilizar la información, configurar la red Wi-Fi propia o reiniciar el dispositivo con alguna configuración anterior.

4 Análisis

Como se detalló anteriormente los entornos con dispositivos IoT que intercambian información crítica para el entorno pueden ser vulnerables a modificaciones, para lo cual se realizó un análisis de posibles vulnerabilidades tanto del hardware como del software.

En una primera etapa se analizaron las posibles vulnerabilidades de hardware, en este sentido se consideraron los aspectos físicos del dispositivo. La evaluación incluyó las consecuencias que provocarían las modificaciones y el comportamiento del dispositivo. De dicha evaluación se tuvieron en cuenta aspectos tales como el acceso a la recalibración, la modificación del programa que permite sensar, acceso físico al botón de apagado de la alarma.

Se encontraron cuatro vulnerabilidades de hardware, dos de ellas relacionadas con el modo en el que se calibra el dispositivo lo que permite que los valores límites sean erróneos y por consecuencia se encienda la luz indicadora incorrecta. Las otras dos vulnerabilidades tienen que ver con puertos y botones específicos del dispositivo que pueden ser manipulados si un atacante tiene acceso físico al mismo.

Estos casos de vulnerabilidades provocarían las siguientes consecuencias:

- En caso que se recalibre el dispositivo para que tome niveles concentrados de CO2 como niveles normales podría provocar que no detecte saturación del aire cuando debería hacerlo. Este caso se conoce como un falso negativo dado que no genera una alerta porque considera como normales valores que no corresponden.
- En caso que se recalibre el dispositivo para que tome niveles demasiado bajos de CO2 como niveles normales podría provocar que la alarma suene, aunque los niveles de CO2 no sean altos. Este caso se considera un falso positivo, dado que estaría alertando que los niveles de dióxido son peligrosos cuando no lo son.

En cuanto al acceso físico a diferentes periféricos del dispositivo las posibles consecuencias son:

- El acceso al puerto USB podría provocar la reescritura del programa dado, que al estar a simple vista, y no solicitar contraseña ni validación para hacerlo, facilita su uso malicioso para re-configurar o cambiar el código fuente. En caso que esta acción se realice podría provocar que el dispositivo

no realice las funcionalidades para lo cual fue programado, o en su defecto con un funcionamiento erróneo o malintencionado.

- En el caso del botón de silenciado que apaga la alarma al instante, una persona podría apagarla de forma casi instantánea y de esta forma las personas presentes en el ambiente no advertirían del peligro de la situación.

En una segunda etapa se realizó el análisis de las vulnerabilidades de software, para lo cual se evaluaron los protocolos y servicios utilizados por el dispositivo mediante capturas de tráfico de red a través de técnicas de sniffing. Durante el análisis, se evaluaron diferentes aspectos, tales como los protocolos de la capa de aplicación utilizados, la seguridad de las contraseñas y el método de autenticación para habilitar la red de configuración.

Cabe mencionar que la cantidad de tráfico presente en los entornos de uso de los dispositivos y la frecuencia en que se configura los mismos pueden dificultar el acceso al tráfico de un dispositivo en particular.

En esta etapa al momento de investigar el modo de autenticación, se pudo determinar a través de las capturas que se utilizaba el protocolo WPA2 para las redes propias de Wi-Fi (RedA y Config_RedA) y el protocolo WWW-Authenticate [16], a través de un popup desde el sitio web, para poder ingresar a la red de configuración del dispositivo IoT para hacer modificaciones. En caso de que las credenciales ingresadas por el usuario sean las correctas, el dispositivo se desconectará de la red actual y abrirá la red de configuraciones.

Se encontraron cuatro vulnerabilidades de software, dos de ellas tienen que ver con el uso de credenciales por defecto. Las dos vulnerabilidades restantes se relacionan con el uso de protocolos inseguros.

El uso de credenciales por defecto se da tanto en el acceso a las redes propias como en el acceso a la configuración a través del protocolo WWW-Authenticate. Dichas contraseñas se encuentran establecidas y no es posible modificarlas. En el caso de las credenciales utilizadas en el protocolo WWW-Authenticate, se configuraron un usuario y contraseña comunes y no permiten su modificación desde el sistema, lo cual genera que sean fácilmente descubiertas en un ataque por fuerza bruta o diccionario. En el caso de las redes inalámbricas, la contraseña y nombres de las redes configuradas en el prototipo si bien no son comunes, serán las mismas utilizadas en todos los medidores de CO2. Esto trae como consecuencia que quien conoce o descubre la clave de uno de ellos puede acceder a todos los medidores, aunque no esté autorizado a ello.

Como se describió anteriormente estas configuraciones seleccionadas generan que sean más predecibles las contraseñas y permite su acceso a través de ataques por diccionario o fuerza bruta.

Respecto al uso de protocolos inseguros, el análisis se centró en el tipo de autenticación utilizado, el protocolo WWW-Authenticate base, que se implementa a través del intercambio de los datos dentro de las cabeceras del paquete, lo cual permitiría descifrar la contraseña por medio de un ataque de diccionario o fuerza bruta sobre dichas cabeceras. Por otra parte, al utilizar HTTP y WebSocket [17], protocolos que no encriptan la información, esto facilita el acceso a la información transmitida y por lo tanto a las credenciales de configuración.

5 Conclusiones

Este artículo presenta un caso particular de la implementación de dispositivos IoT, las características del prototipo, un análisis realizado con posibles vulnerabilidades y propuestas de mitigación. Además, se detallan la forma de comunicación entre las diferentes partes del escenario y las consecuencias que podrían suceder en los diferentes casos de vulnerabilidad. En cuanto a las vulnerabilidades de hardware se detallan los cuidados a nivel del dispositivo, su alcance físico y los periféricos que podrían generar intervenciones externas. Por lo tanto, se recomienda deshabilitar los puertos mediante un bloqueo lógico o físico, modificar el comportamiento del dispositivo cuando se interactúa con los botones y posicionar el dispositivo en un lugar que no sea de fácil acceso para el público, pero en el cual pueda seguir cumpliendo su funcionalidad.

Con respecto a las vulnerabilidades de software se recomienda utilizar protocolos seguros para prevenir los ataques más comunes, establecer una política de contraseñas fuertes que a través del mismo sistema fuercen al administrador el cambio de la misma luego de un determinado tiempo. Por último, el desarrollo del programa que se ejecuta localmente en la placa y lleva a cabo la configuración, reforzar el modo de autenticación utilizando protocolos que eviten el fácil acceso a la información transmitida.

A partir de esta investigación se puede concluir que existen similitudes y particularidades en el análisis y mitigación de vulnerabilidades de arquitecturas de IoT respecto a arquitecturas tradicionales. En cuanto a las metodologías y herramientas para detectar vulnerabilidades, es posible utilizar las mismas en ambos casos.

Si hablamos de detección de vulnerabilidades en sistemas de IoT, tenemos que tener presentes los mecanismos de seguridad implementados en los protocolos de transmisión de información, al igual que en otras arquitecturas. También resulta similar el análisis de la seguridad de los servicios, como ser el mecanismo de autenticación y la gestión de claves, así como la seguridad de su configuración por defecto. Mientras que, si pensamos en vulnerabilidades de los dispositivos y problemas de seguridad física, hay que tener en cuenta características inherentes a los sistemas de IoT, donde los dispositivos suelen residir en lugares públicos y abiertos, y además tener limitaciones de hardware que dificultan su protección y su configuración segura. Por otro lado, al momento de evaluar las medidas para lograr la mayor seguridad en los dispositivos, se debe tener en cuenta las capacidades de los dispositivos para la implementación de protocolos más seguros y cómo esto podría aumentar el retardo y el consumo de energía que provocan.

Referencias

[1]Smart cities: Background paper. GOV.UK. Recuperado 19 de julio de 2022, de https://www.gov.uk/government/publications/smart-cities-background-paper

[2]Forecast: The Internet of Things, Worldwide, 2013. (s. f.). Gartner. Recuperado 21 de julio de 2022, de https://www.gartner.com/en/documents/2625419

[3]Blanco-Novoa et al., (2017). An Open-Source IoT Power Outlet System for Scheduling Appliance Operation Intervals Based on Real-Time Electricity Cost. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2017.141

[4]Díaz, F. J. et al., (2017, abril). Estrategias de IOT para lograr ciudades digitales seguras, más inclusivas y sustentables. XIX Workshop de Investigadores en Ciencias de la Computación (WICC 2017, ITBA, Buenos Aires). http://sedici.unlp.edu.ar/handle/10915/62410

[5]Díaz, F. J. et al., (2021). Investigación en ciberseguridad en un año de pandemia. XXIII Workshop de Investigadores en Ciencias de la Computación (WICC 2021, Chilecito, La Rioja). http://sedici.unlp.edu.ar/handle/10915/120528

[6]Monzón, G. et al., (2019). Modelo de seguridad IoT. XXV Congreso Argentino de Ciencias de la Computación (CACIC) (Universidad Nacional de Río Cuarto, Córdoba, 14 al 18 de octubre de 2019). http://sedici.unlp.edu.ar/handle/10915/91363

[7]Pertini, B. (2017). Análisis y mejoras de seguridad a una aplicación prototipo en IoT [Tesis, Universidad Nacional de La Plata]. http://sedici.unlp.edu.ar/handle/10915/72059

[8] Presentación del Proyecto "Hackeamos para construir robot seguros" https://www.youtube.com/watch?v=XHICnjsjcVs. Último acceso 27 de julio.

[9] Proyecto del LINTI subsidiado por la OEA, año 2021-2022. https://www.youtube.com/watch?v=AuhPA45LYkQ&t=7s

[10] Antonio Liñán Colina, Alvaro Vives, Marco Zennaro, Antoine Bagula, Ermanno Pietrosemoli. Internet of Things IN 5 DAYS. https://archive.org/details/IoT5days. Último acceso 25 de Julio de 2022.

[11] OWASP (Web Open Application Security Project) www.owasp.org. Último acceso: 21 de Julio de 2022.

[12] NIST Cybersecurity for IoT Program. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program. Último acceso: 21 de Julio de 2022.

[13]CIS Controls v8 Internet of Things Companion Guide White paper. Recuperado 21 de julio de 2022, de https://www.cisecurity.org/white-papers/cis-controls-v8-internet-of-things-companion-guide/

[14]IoT Security Foundation. https://www.iotsecurityfoundation.org/. Último acceso 27 de julio de 2022.

[15]NodeMCU Official Website. Disponible online: http://www.nodemcu.com. Último acceso: 21 de Julio de 2022.

[16]WWW-Authenticate. https://developer.mozilla.org/es/docs/Web/HTTP/Headers/WWW-Authenticate. Último acceso: 1 de Agosto de 2022

[17]Request for Comments: 6455. The WebSocket Protocol. https://datatracker.ietf.org/doc/html/rfc6455. Último acceso: 1 de Agosto de 2022.