UNIVERSIDAD
REY JUAN CARLOS

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

GRADO EN INGENIERÍA EN TECNOLOGÍAS DE LA TELECOMUNICACIÓN

Curso Académico 2018/2019

Trabajo Fin de Grado

IMPLEMENTACIÓN DEL PROTOCOLO DE AUTORIZACIÓN OAUTH2

Autor : Pedro Tello Sánchez

Tutor : Pedro De Las Heras Quirós

Trabajo Fin de Grado

Implementación del Protocolo de Autorización oAUTH2

Autor : Pedro Tello Sánchez

Tutor : Pedro de las Heras Quirós

La defensa del presente Proyecto Fin de Carrera se realizó el día de de 2019, siendo calificada por el siguiente tribunal:

Presidente:

Secretario:

Vocal:

y habiendo obtenido la siguiente calificación:

Calificación:

Fuenlabrada, a de de 20XX

Dedicado a

mi familia / mi abuelo / mi abuela

II

Agradecimientos

Aquí vienen los agradecimientos... Aunque está bien acordarse de la pareja, no hay que olvidarse de dar las gracias a tu madre, que aunque a veces no lo parezca disfrutará tanto de tus logros como tú... Además, la pareja quizás no sea para siempre, pero tu madre sí.

Resumen

Aquí viene un resumen del proyecto. Ha de constar de tres o cuatro párrafos, donde se presente de manera clara y concisa de qué va el proyecto. Han de quedar respondidas las siguientes preguntas:

- ¿De qué va este proyecto? ¿Cuál es su objetivo principal?
- ¿Cómo se ha realizado? ¿Qué tecnologías están involucradas?
- ¿En qué contexto se ha realizado el proyecto? ¿Es un proyecto dentro de un marco general?

Lo mejor es escribir el resumen al final.

Summary

Here comes a translation of the “Resumen” into English. Please, double check it for correct grammar and spelling. As it is the translation of the “Resumen”, which is supposed to be written at the end, this as well should be filled out just before submitting.

Índice general

Índice de figuras

Capítulo 1

Introducción

Este Trabajo Fin de Grado se desarrolla en el ámbito de la seguridad y la preservación de la confidencialidad en Internet. En este capítulo introduciremos los conceptos y tecnologías utilizadas a la vez que se presentará el esquema general de la custodia de la información.

1.1. Historia

Internet se ha convertido en el centro de nuestras vidas. Según un estudio realizado por la compañía Brandwatch [1] en Abril de 2018 la población mundial era de 7.8 mil millones de personas de los cuales 4.2 mil millones de personas eran usuarios de Internet y 3.03 mil millones eran usuarios de redes sociales y/o estaban registrados en páginas web.

Con tal magnitud de usuarios generando datos en poco tiempo, se llegó a la conclusión, de que la información de los usuarios contenida en diferentes sitios web, podía ser de valor para otras entidades y se comenzaron a crear servicios que permitían el envío de determinada información bajo autorización del propietario de la misma. Así fue como nacieron las API que ofrecían servicios y las Aplicaciones que podrían consumir los mismos.

El problema surgió cuando para acceder a la información de un determinado usuario era necesario suministrar las credenciales de acceso de dicho usuario. Esa información era crítica y bajo ningún concepto se podría suministrar a alguien que no fuera la API o el usuario. Por tanto se necesitaba conseguir que los usuarios, propietarios de los datos, pudieran disponer de un protocolo seguro mediante el cuál facilitar las credenciales únicamente a la API. Así se llegó

[1] `www.brandwatch.com`

a la conclusión de que era necesario encontrar métodos de autenticación que no pusieran en peligro la información personal del usuario a la vez que concedieran los permisos necesarios de autorización para acceder a la información específica que quisiera el usuario.

A lo largo de los años han ido surgiendo diferentes tecnologías que iban proporcionando soluciones tanto al concepto de autorización como al concepto de autenticación.

1.2. Diferencias entre Autorización y Autenticación

Son dos conceptos se suelen confundir con bastante frecuencia. Mientras que la autenticación se enfoca en determinar que el usuario es quien dice ser, la autorización se encarga de controlar qué acciones ese usuario puede realizar.

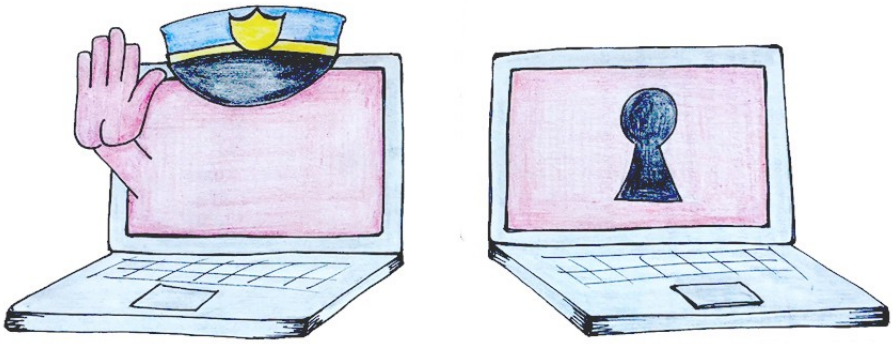

Figura 1.1: Autorización VS Autenticación

1.2.1. Autorización

La autorización se encarga de determinar si tenemos autoridad para hacer algo. Pensemos por ejemplo en las aplicaciones móviles en las que existe una versión Lite (gratuita) y una

versión Pro (de pago). Un usuario gratuito está autorizado a acceder a un conjunto limitado de funcionalidades y no está autorizado a otras funcionalidades, mientras no pague la suscripción y se convierta en usuario Premium.

Cada vez que un usuario intenta acceder a una funcionalidad, la aplicación realiza un control para determinar si puede hacerlo o no. En segundo plano, lo que está ocurriendo es un proceso de autorización. Siempre que el usuario acceda a recursos para los que tiene permisos, no habrá problema. Sin embargo, en cuanto el usuario intente acceder a un recurso que solo está disponible para la versión Pro, se le denegará el permiso y comunmente se le invita a unirse al paquete Premium.

1.2.2. Autenticación

La autenticación se define como el proceso mediante el cual se verifica que un individuo, es quien dice ser. Un ejemplo sería, por ejemplo, el proceso de autenticación que realiza Google. Cuando se inicia sesión introduciendo un correo electrónico y contraseña estamos autenticándonos. Google está comprobando que la contraseña introducida coincide con la contraseña que se asoció a mi correo electrónico en el momento del registro. Si la contraseña coincide con el correo podremos acceder a la aplicación, sin embargo, si la contraseña no coincide con el correo, Google no permitirá el inicio de sesión porque no se puede asegurar que la persona sea quien dice ser.

Debido a que la posibilidad de que nos roben la contraseña existe, en los últimos años ha surgido la autenticación de dos factores. Dicha autenticación consiste en agregar un segundo paso para verificar que la persona es quien dice ser. Entonces, no solo se necesitaría la contraseña sino que se requeriría un paso adicional. La manera más común de realizar dicha autenticación consiste en enviar un mensaje al correo electrónico desde el cual se está intentando acceder o mediante el envío de un código al teléfono móvil de contacto.

Autenticación mediante Certificados Electrónicos

A partir de los avances tecnológicos actuales podemos predecir que las contraseñas ya no son un método confiable de autenticación de usuario. Este problema, combinado con la creciente amenaza de máquinas malintencionadas, hace que muchos expertos en TI se pregunten como

pueden asegurarse de que solo los usuarios y dispositivos aprobados tengan acceso. La solución a este problema lo podemos encontrar en los certificados electrónicos.

La autenticación basada en certificados es el nombre que se le da a utilizar un Certificado Digital para identificar a un usuario, máquina o dispositivo antes de otorgar acceso a un recurso, red, aplicación, etc. En el caso de la autenticación de usuario, a menudo se implementa en conjunto con métodos tradicionales como nombre de usuario y contraseña. A diferencia de algunas soluciones que solo funcionan para usuarios, como la biométrica y las contraseñas de un solo uso, la autenticación mediante certificado se puede utilizar para cualquier gestión final: usuarios, máquinas, dispositivos e incluso para gestionar la tecnología creciente de Internet of Things.

1.3. Mecanismos de Autorización y Autenticación

1.3.1. SAML

1.3.2. OpenID Connect

1.3.3. oAuth 2.0

El estandar OAuth 2.0 (RFC 6749) es un framework de autorización que permite controlar el acceso por parte de las aplicaciones a los datos de los usuarios sin tener que proporcionar las credenciales. Según el estandar, el marco de autorización de OAuth 2.0 permite que una aplicación de terceros obtenga acceso limitado a un servicio HTTP, ya sea en nombre de un propietario de recursos mediante la organización de una interacción de aprobación entre el propietario del recurso y el servicio HTTP, o permitiendo a la aplicación de terceros obtener acceso en su propio nombre.

1.4. Estructura de la memoria

En esta sección se debería introducir la esctura de la memoria. Así:

- En el primer capítulo se hace una intro al proyecto.
- En el capítulo 2 (ojo, otra referencia automática) se muestran los objetivos del proyecto.

- Estado del Arte: Tecnologías que vamos a usar en el proyecto.
- Diseño e implementación: Aquí viene todo lo que has hecho tú (tecnológicamente). Puedes entrar hasta el detalle. Es la parte más importante de la memoria, porque describe lo que has hecho tú. Eso sí, normalmente aconsejo no poner código, sino diagramas.
- Resultados: En este capítulo se incluyen los resultados de tu trabajo fin de grado.
- Conclusiones: Esta sección es la sección espejo de las dos primeras del capítulo de objetivos, donde se planteaba el objetivo general y se elaboraban los específicos. Es aquí donde hay que debatir qué se ha conseguido y qué no. Cuando algo no se ha conseguido, se ha de justificar, en términos de qué problemas se han encontrado y qué medidas se han tomado para mitigar esos problemas.

Capítulo 2

Objetivos

2.1. Objetivo general

Aquí vendría el objetivo general en una frase: Mi trabajo fin de grado consiste en crear de una herramienta de análisis de los comentarios jocosos en repositorios de software libre alojados en la plataforma GitHub.

Recuerda que los objetivos siempre vienen en infinitivo.

2.2. Objetivos específicos

Los objetivos específicos se pueden entender como las tareas en las que se ha desglosado el objetivo general. Y, sí, también vienen en infinitivo.

2.3. Planificación temporal

A mí me gusta que aquí pongáis una descripción de lo que os ha llevado realizar el trabajo. Hay gente que añade un diagrama de GANTT. Lo importante es que quede claro cuánto tiempo llevas (tiempo natural, p.ej., 6 meses) y a qué nivel de esfuerzo (p.ej., principalmente los fines de semana).

Capítulo 3

Estado del arte

Descripción de las tecnologías que utilizas en tu trabajo. Con dos o tres párrafos por cada tecnología, vale. Se supone que aquí viene todo lo que no has hecho tú.

Puedes citar libros, como el de Bonabeau et al. sobre procesos estigmérgicos [1].

También existe la posibilidad de poner notas al pie de página, por ejemplo, una para indicarte que visite la página de LibreSoft[1].

3.1. Sección 1

Hemos hablado de cómo incluir figuras. Pero no hemos dicho nada de tablas. A mí me gustan las tablas. Mucho. Aquí un ejemplo de tabla, la Tabla 3.1.

[1] `http://www.libresoft.es`

1	2	3
4	5	6
7	8	9

Cuadro 3.1: Ejemplo de tabla

Capítulo 4

Diseño e implementación

Aquí viene todo lo que has hecho tú (tecnológicamente). Puedes entrar hasta el detalle. Es la parte más importante de la memoria, porque describe lo que has hecho tú. Eso sí, normalmente aconsejo no poner código, sino diagramas.

4.1. Arquitectura general

Si tu proyecto es un software, siempre es bueno poner la arquitectura (que es cómo se estructura tu programa a "vista de pájaro").

Por ejemplo, puedes verlo en la figura 4.1.

Si utilizas una base de datos, no te olvides de incluir también un diagrama de entidad-relación.

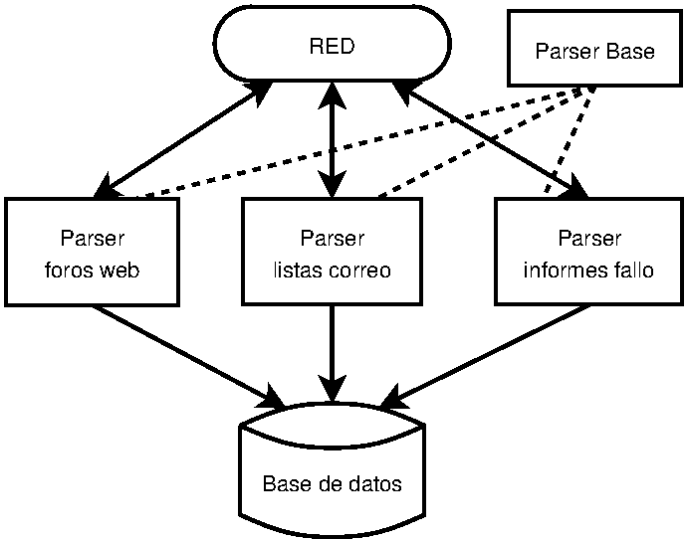

Figura 4.1: Estructura del parser básico

Capítulo 5

Resultados

En este capítulo se incluyen los resultados de tu trabajo fin de grado.

Si es una herramienta de análisis lo que has realizado, aquí puedes poner ejemplos de haberla utilizado para que se vea su utilidad.

Capítulo 6

Conclusiones

6.1. Consecución de objetivos

Esta sección es la sección espejo de las dos primeras del capítulo de objetivos, donde se planteaba el objetivo general y se elaboraban los específicos.

Es aquí donde hay que debatir qué se ha conseguido y qué no. Cuando algo no se ha conseguido, se ha de justificar, en términos de qué problemas se han encontrado y qué medidas se han tomado para mitigar esos problemas.

6.2. Aplicación de lo aprendido

Aquí viene lo que has aprendido durante el Grado/Máster y que has aplicado en el TFG/TFM. Una buena idea es poner las asignaturas más relacionadas y comentar en un párrafo los conocimientos y habilidades puestos en práctica.

1. a
2. b

6.3. Lecciones aprendidas

Aquí viene lo que has aprendido en el Trabajo Fin de Grado/Máster.

1. a

2. b

6.4. Trabajos futuros

Ningún software se termina, así que aquí vienen ideas y funcionalidades que estaría bien tener implementadas en el futuro.

Es un apartado que sirve para dar ideas de cara a futuros TFGs/TFMs.

Apéndice A

Manual de usuario

Bibliografía

[1] E. Bonabeau, M. Dorigo, and G. Theraulaz. *Swarm Intelligence: From Natural to Articial Systems*. Oxford University Press, Inc., 1999.