



TRABAJO FIN DE GRADO

GRADO EN INGENIERÍA INFORMÁTICA

TFG - DASIoT

DASIoT: Desarrollo y Auditoría de Seguridad para prototipo de dispositivos IoT

Autor

Luis Aróstegui Ruiz

Directores

José Manuel Soto Hidalgo

Alberto Guillén Perales



ESCUELA TÉCNICA SUPERIOR DE INGENIERÍAS INFORMÁTICA Y DE
TELECOMUNICACIÓN

Granada, 21 de marzo de 2022

TFG - DASIoT: Desarrollo y Auditoría de Seguridad para prototipo de dispositivos IoT

Luis Aróstegui Ruiz

Palabras clave: Internet de las Cosas, Seguridad

Resumen

En el contexto de IoT, hay un ecosistema de entornos de desarrollo específicos. En este TFG se hará uso de alguno de ellos para llevar a cabo la implementación de un dispositivo IoT y analizar los potenciales problemas de seguridad que pueden aparecer durante la etapa de implementación.

Project Title: Project Subtitle

First name, Family name (student)

Keywords: Keyword1, Keyword2, Keyword3,

Abstract

Write here the abstract in English.

Yo, **Nombre Apellido1 Apellido2**, alumno de la titulación **TITULACIÓN de la Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación de la Universidad de Granada**, con DNI XXXXXXXXX, autorizo la ubicación de la siguiente copia de mi Trabajo Fin de Grado en la biblioteca del centro para que pueda ser consultada por las personas que lo deseen.

Fdo: Nombre Apellido1 Apellido2

Granada a X de mes de 201 .

D. **Nombre Apellido1 Apellido2 (tutor1)**, Profesor del Área de XXXX del Departamento YYYY de la Universidad de Granada.

D. **Nombre Apellido1 Apellido2 (tutor2)**, Profesor del Área de XXXX del Departamento YYYY de la Universidad de Granada.

Informan:

Que el presente trabajo, titulado ***Título del proyecto, Subtítulo del proyecto***, ha sido realizado bajo su supervisión por **Nombre Apellido1 Apellido2 (alumno)**, y autorizamos la defensa de dicho trabajo ante el tribunal que corresponda.

Y para que conste, expiden y firman el presente informe en Granada a X de mes de 201 .

Los directores:

Nombre Apellido1 Apellido2 (tutor1)
(tutor2)

Nombre Apellido1 Apellido2

Agradecimientos

Poner aquí agradecimientos...

Índice general

1. Introducción	15
1.1. Descripción y contexto	15
1.2. Motivación	16
1.3. Objetivos	16
1.3.1. Objetivos específicos	17
2. Planificación	19
2.1. Planificación a priori	19
2.1.1. Etapas de desarrollo	19
2.1.2. Diagrama de Gantt	19
3. Análisis del problema	21
4. Diseño	23
5. Implementación	25
6. Pruebas	27
7. Conclusiones y trabajos futuros	29

Índice de figuras

2.1. Fechas y duración de cada etapa del diagrama de Gantt	20
2.2. Diagrama de Gantt. Gráfico.	20

Luis Aróstegui Ruiz

Índice de tablas

CAPÍTULO 1

Introducción

1.1. Descripción y contexto

El Internet de las Cosas, o IoT, es un sistema de dispositivos informáticos, máquinas mecánicas y digitales, objetos, animales o personas interrelacionados que cuentan con identificadores únicos (UID) y la capacidad de transferir datos a través de una red sin que sea necesaria la interacción entre personas o entre ordenadores.

Una “cosa” en el Internet de las Cosas puede ser una persona con un implante de monitor cardíaco, un animal de granja con un transpondedor de biochip, un automóvil que tiene sensores incorporados para alertar al conductor cuando la presión de los neumáticos es baja o cualquier otro objeto natural o artificial al que se le pueda asignar una dirección de Protocolo de Internet (IP) y que sea capaz de transferir datos a través de una red.

Cada vez más, las organizaciones de diversos sectores utilizan el IoT para operar de forma más eficiente, comprender mejor a los clientes para ofrecerles un mejor servicio, mejorar la toma de decisiones y aumentar el valor del negocio.

El concepto de *Internet of Things* fue propuesto en 1999 por el laboratorio de identificación automática del Instituto Tecnológico de Massachusetts (MIT). La UIT lo dio a conocer en 2005, empezando por China. El IoT puede definirse como “*datos y dispositivos continuamente disponibles a través de Internet*”. La interconexión de “cosas” (objetos) que pueden dirigirse de forma inequívoca y las redes heterogéneas constituyen el IoT. La identificación por radiofrecuencia (RFID), los sensores, las tecnologías inteligentes y las nanotecnologías son los

principales contribuyentes a al IoT para una variedad de servicios.

Con la drástica reducción del coste de sensores y con la evolución de tecnologías como el ancho de banda, el procesamiento, los teléfonos inteligentes, la migración hacia el IPv6 y el 5G se está facilitando la adopción del IoT.

El IoT también ve todo como lo mismo, sin discriminar entre humanos y máquinas. Las “cosas” incluyen a los usuarios finales, los centros de datos (DC), las unidades de procesamiento, los teléfonos inteligentes, las tabletas, el Bluetooth, el ZigBee, la Asociación de Datos por Infrarrojos (IrDA), la banda ultraancho (UWB), las redes celulares, las redes Wi-Fi, los DC de comunicación de campo cercano (NFC), la RFID y sus etiquetas, los sensores y los chips, los equipos domésticos, los relojes de pulsera, los vehículos y las puertas de las casas.

1.2. Motivación

Las personas de todo el mundo están ya preparadas para disfrutar de las ventajas del Internet de las cosas (IoT). El IoT lo incorpora todo, desde el sensor corporal hasta la computación en la nube. Comprende los principales tipos de redes, como la distribuida, la de red, la ubicua y la vehicular, que han conquistado el mundo de la informática durante una década. Desde el estacionamiento de vehículos a su seguimiento, de la introducción de datos de pacientes a la observación de los pacientes a la observación de los pacientes, de la atención a los niños a la atención a los ancianos, de las tarjetas inteligentes a las tarjetas de campo cercano, los sensores están haciendo sentir su presencia. Los sensores desempeñan un papel fundamental en el IoT.

El IoT funciona en redes y estándares heterogéneos. Excepcionalmente, ninguna red está libre de amenazas y vulnerabilidades de seguridad. Cada una de las capas del IoT está expuesta a diferentes tipos de amenazas. Este proyecto se centra en las posibles amenazas que hay que abordar y mitigar para conseguir una comunicación segura en el IoT.

En otras palabras, el IoT combina “lo real y lo virtual” en cualquier lugar y en cualquier momento, atrayendo la atención tanto de desarrolladores como de ciberdelincuentes. Inevitablemente, dejar los dispositivos sin intervención humana durante un largo periodo podría dar lugar a robos.

1.3. Objetivos

El principal objetivo de este proyecto es hacer uso de un entorno de desarrollo específico para llevar a cabo una implementación de un dispositivo IoT y analizar

los potenciales problemas de seguridad que pueden aparecer durante la etapa de implementación.

1.3.1. Objetivos específicos

- **OE.1:** Estudiar los distintos entornos de desarrollo para IoT y analizar funcionalidades y propiedades que se ajusten al proyecto.
- **OE.2:** Desarrollar un prototipo de aplicación para IoT utilizando un framework de desarrollo.
- **OE.3:** Explotación de una vulnerabilidad a nivel de dispositivo, protocolo, SO, aplicación o HW.

CAPÍTULO 2

Planificación

2.1. Planificación a priori

Se trata de planificar como se espera desarrollar el proyecto en el tiempo, para ello se va a hacer uso de un diagrama de Gantt donde se va a proporcionar una vista general de las tareas programadas, estas tareas tendrán que completarse en unas fechas estipuladas. Para poder realizar el digrama se tienen que indicar las etapas de desarrollo del proyecto.

2.1.1. Etapas de desarrollo

- **1ª etapa:** Revisar entornos de desarrollo para IoT.
- **2ª etapa:** Desarrollar aplicación para IoT.
- **3ª etapa:** Explotación de una vulnerabilidad.
- **4ª etapa:** Documentación.

2.1.2. Diagrama de Gantt

De los 3 meses y medios a que se van a dedicar al proyecto, en todos ellos se va a desarrollar las etapas indicadas anteriormente. Se muestra la fecha de inicio y de fin de cada etapa.

Etapas del desarrollo	Fecha de comienzo	Fecha de finalización
Documentación del proyecto	9 de Marzo	23 de Junio
Revisar entornos de desarrollo IoT	21 de Marzo	30 de Marzo
Desarrollar aplicación para IoT	31 de Marzo	5 de Mayo
Explotar vulnerabilidad	6 de Mayo	15 de Junio

Tabla 2.1: Tabla con la organización temporal del proyecto.

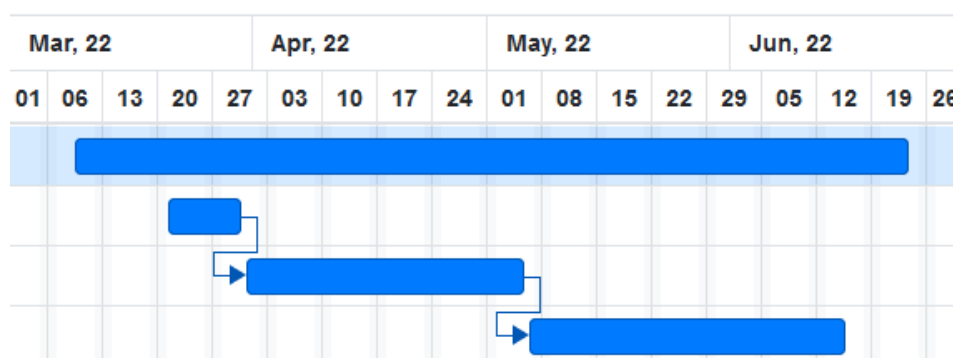


Figura 2.1: Diagrama de Gantt. Gráfico.

Este gráfico corresponde con la duración de cada etapa, comenzando con la documentación. También se indica que hay etapas que para que estas se puedan empezar a desarrollar necesitan que la anterior este terminada, es el caso de la etapa de *Desarrollo de la aplicación* y de *Explotación de una vulnerabilidad*.

CAPÍTULO 3

Análisis del problema

CAPÍTULO 4

Diseño

CAPÍTULO 5

Implementación

Para citar una referencia bibliográfica: [?]

CAPÍTULO 6

Pruebas

CAPÍTULO 7

Conclusiones y trabajos futuros
