How p2p framework can help mitigate trust and security risks of IoT applications

A .onion based framework to address trust and privacy issues for the IoT

Pablo R. Grande
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Protocolos y aplicaciones de seguridad

Silvia Puglisi
Victor García Font
Fecha Entrega

Licencias alternativas (elegir alguna de las siguientes y sustituir la de la página anterior)

A) Creative Commons:

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-SinObraDerivada 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento-CompartirIgual 3.0 España de Creative Commons

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

B) GNU Free Documentation License (GNU FDL)

Copyright © AÑO TU-NOMBRE.

Permission is granted to copy, distribute and/or modify this document under the terms of the

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Descripción del trabajo*
Nombre del autor:	*Nombre y dos apellidos*
Nombre del consultor/a:	*Nombre y dos apellidos*
Nombre del PRA:	*Nombre y dos apellidos*
Fecha de entrega (mm/aaaa):	MM/AAAA
Titulación:	*Plan de estudios del estudiante*
Área del Trabajo Final:	*El nombre de la asignatura de TF*
Idioma del trabajo:	
Palabras clave	*Máximo 3 palabras clave, validadas por el director del trabajo (dadas por los estudiantes o en base a listados, tesauros, etc.)*
Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*	

Abstract (in English, 250 words or less):

Índice

Lista de figuras

No se encuentran elementos de tabla de ilustraciones.

.1. Introducción

.1.1 Contexto y justificación del Trabajo

El internet of things (IoT) espera integrar un gran número de sensores a internet y cuyas aplicaciones son aglutinadas en su infraestructura y reutilizarse para distintos propósitos. Sin embargo, la privacidad en estas comunicaciones supone un reto para muchas aplicaciones debido a que muchos de estos dispositivos recogen datos de índole personal sobre individuos a través de sensores de forma desconocida para ellos. Además, estos dispositivos tienen un diseño específico y carecen de capacidades de procesamiento requeridas para llevar a cabo tareas de seguridad. Por tanto, hay una gran cantidad de datos sensibles que circulan por la red sin ningún tipo de garantía de privacidad lo que supone un gran riesgo para los dispositivos y para sus usuarios.

.1.2 Objetivos del Trabajo

El objetivo de este proyecto es desarrollar una arquitectura o framework capaz de establecer comunicaciones entre dispositivos IoT manteniendo la privacidad de los mismos. El framework deberá ser capaz de sentar las bases de una arquitectura para el desarrollo de aplicaciones que garanticen la privacidad entre las comunicaciones de los dispositivos con bajo coste computacional.

Concretamente, los objetivos son:

- Escribir un artículo donde se plantee el estado del arte de los sistemas actuales de comunicación de dispositivos IoT y los problemas de privacidad que plantea.
- Desarrollar un framework p2p que mitigue los riesgos de seguridad identificados en aplicaciones IoT. Este framework hace uso de los servicios .onion y el protocolo Tor.
- Desarrollar una aplicación de muestra siguiendo la arquitectura propuesta por el framework. Esta aplicación de ejemplo permitirá a varios dispositivos IoT compartir datos de manera anónima mediante servicios .onion.
- Aprender sobre el protocolo Tor y sevicios .onion y sus posibles aplicaciones.

.1.3 Enfoque y método seguido

El enfoque seguido para este trabajo consiste en el análisis de arquitecturas existentes de comunicaciones privadas o no entre dispositivos IoT, de sus carencias y limitaciones y a partir de ahí desarrollar un producto nuevo.
Dado que uno de los objetivos de este trabajo consiste en confeccionar un artículo, el método seguido requiere primero de un análisis del estado del arte de la seguridad aplcicada a IoT con énfasis en la privacidad. Posteriormente se propondrá una arquitectura alternativa o una que aporte mejoras a las ya existentes a nivel teórico. Luego se desarrollará una aplicación que implemente los patrones del framework y que, efectivamente, permita la comunicación con cierto grado de privacidad entre dispositivos IoT. A continuación, se propondrán una serie de pruebas y experimentos con la finalidad de obtener resultados que muestren la efectividad del framework y su aplicación. Finalmente, los resultados serán recogidos y contrastados para ser plasmados en un artículo junto con la especificaciones del framework.

.1.4 Planificación del Trabajo

Para el desarrollo de este trabajo se necesitan ciertos materiales para desarrollar y elaborar experimentos que comprueben la efectividad del framework.

Los recursos materiales son:

- Dispositivos IoT
- Un dispositivo más potente capaz de ejecutar Tor

Otros recursos:

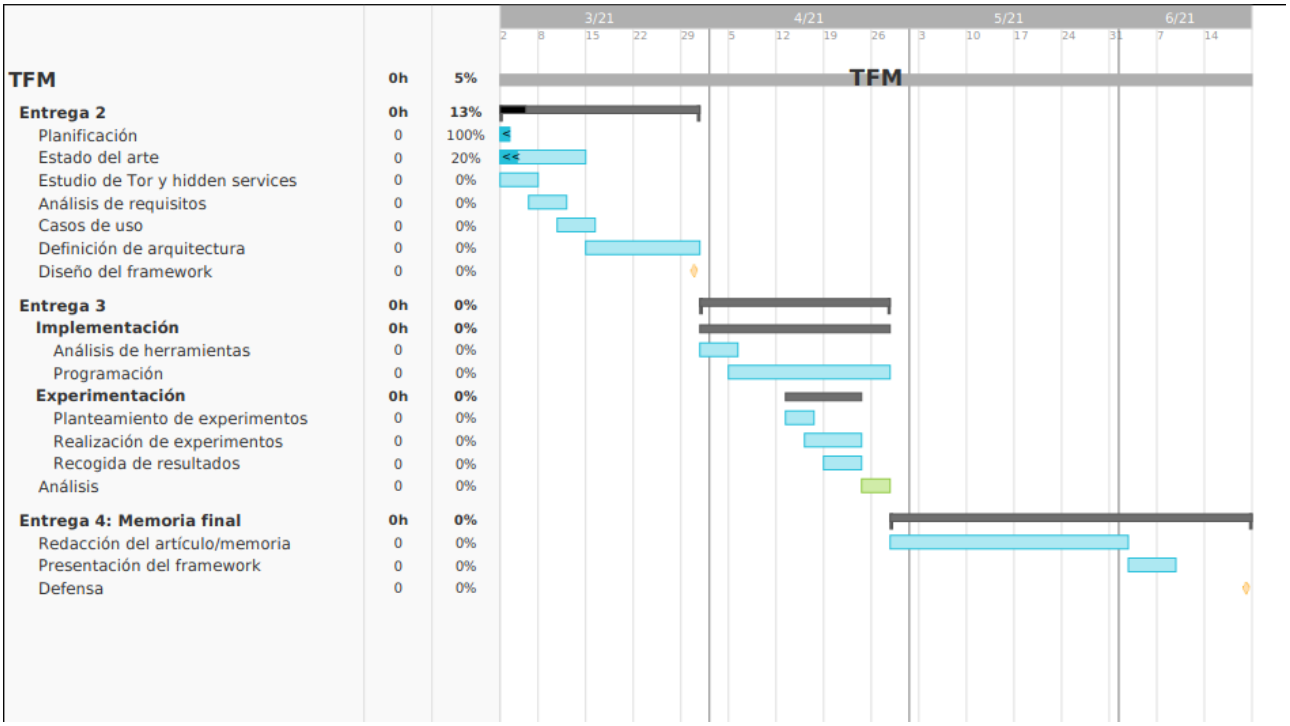
- Acceso a distintos recursos bibliográficos
- Herramientas de diseño y desarrollo de software

La planificación termporal se divide en 3 entregas:

- Entrega 2 (30/3):
  Esta entrega consiste en las tareas de análisis y diseño del trabajo a entregar
  - Estudio del estado del arte (12/3): Mediante el acceso a recursos bibliográficos y otras fuentes se hará un esbozo contrastable del trabajo relacionado con el problema a resolver y qué otras soluciones existen
  - Estudio de Tor y hidden services (5/3): Tor es un eje central para este proyecto y es esencial entender su arquitectura y funcionamiento.
  - Análisis de requisitos (10/3).
  - Casos de uso (15/3).
  - Definición de arquitectura (30/3): En este paso estaremos en disposición de asentar una propuesta de arquitectura con todos los pasos anteriormente realizados como base.

- Entrega 3 (27/4):
  Esta entrega se basa en realizarun producto final y tangible utilizando la arquitectura propuesta.
  - Implementación (27/4):
    - Análisis de herramientas (5/4): De la misma forma que se hace un estudio del estado del arte en cuanto a diseños e ideas es importante investigar las soluciones tecnológicas que puedan ayudar a solventar el problema planteado.
    - Programación (27/4): Programación de la aplicación siguiendo los requisitos y casos de uso anteriomente realizados. Esta tarea es transversal a la experimentación ya que se hará concurrentemente.
  - Experimentación (22/4)
    - Planteamiento de experimentos (15/4): Realizar una serie de problemas a resolver por la aplicación de forma cuantificable
    - Realización de experimentos (22/4).
    - Recogida de resultados (22/4).
  - Análisis (27/4): Una vez realizados los experimentos y recogidos sus resultados se podrá hacer un análisis que muestren la efectividad del framework y la aplicación frente a problemas reales
- Entrega 4: Memoria final (18/6)
  - Redacción del artículo/memoria (1/6)
  - Presentación del framework (8/6): Prequeña presentación en PowerPoint o similar que sumarice el framework y la aplicación
  - Defensa (18/6)

Diagrama de Gantt:



.1.5 Breve sumario de productos obtenidos

No hay que entrar en detalle: la descripción detallada se hará en el resto de capítulos.

.1.6 Breve descripción de los otros capítulos de la memoria

Explicación de los contenidos de cada capítulo y su relación con el trabajo en global.

.2. Resto de capítulos

En estos capítulos, hay que describir los aspectos más relevantes del diseño y desarrollo del proyecto, así como de los productos obtenidos. **La estructuración de los capítulos puede variar según el tipo de Trabajo**.

En cada apartado es muy importante describir las alternativas posibles, los criterios utilizados para tomar decisiones y la decisión tomada.

En caso de que corresponda, se incluirá un apartado de "Valoración económica del trabajo". Este apartado indicará los gastos asociados al desarrollo y mantenimiento del trabajo, así como los beneficios económicos obtenidos. Hacer un análisis final sobre la viabilidad del producto.

.3. Conclusiones

Este capítulo tiene que incluir:

- Una descripción de las conclusiones del trabajo: ¿Qué lecciones se han aprendido del trabajo?
- Una reflexión crítica sobre el logro de los objetivos planteados inicialmente: ¿Hemos logrado todos los objetivos? Si la respuesta es negativa, ¿por qué motivo?
- Un análisis crítico del seguimiento de la planificación y metodología a lo largo del producto: ¿Se ha seguido la planificación? ¿La metodología prevista ha sido la adecuada? ¿Ha habido que introducir cambios para garantizar el éxito del trabajo? ¿Por qué?
- Las líneas de trabajo futuro que no se han podido explorar en este trabajo y han quedado pendientes.

.4. Glosario

Definición de los términos y acrónimos más relevantes utilizados dentro de la Memoria.

.5. Bibliografía

Lista numerada de las referencias bibliográficas utilizadas dentro de la memoria. En cada lugar donde se utilice una referencia dentro del texto, hay que indicarla citando el número de la referencia, por ejemplo: [7].

Es muy importante incluir **todas** las referencias utilizadas y citarlas apropiadamente, es decir, incluyendo toda la información necesaria para identificar la referencia. La información mínima que hay que incluir según el tipo de referencia es:

- **Libro:** Autores, Título, Edición (si se tercia) Editorial, Ciudad, Año.
- **Artículo de revista:** Autores, Título, Nombre de la Revista, Número de Página inicial y final, Número de la revista / Volumen, Año.
- **Web:** URL y fecha en que se ha visitado.

.6. Anexos

Listado de apartados que son demasiado extensos para incluir dentro de la memoria y tienen un carácter autocontenido (por ejemplo, manuales de usuario, manuales de instalación, etc.)

Dependiente del tipo de trabajo, es posible que no haya que añadir ningún anexo.