

Resumen do Trabajo de Fin de Grao

La generalización del uso de dispositivos USB ha supuesto una nueva vía que posibles atacantes pueden emplear como vector de ataque, tanto para la difusión de software malicioso, como para causar algún tipo de daño en los equipos que sean conectados estos dispositivos USB maliciosos.

En este contexto, esta propuesta de TFG pretende desarrollar los componentes básicos de una plataforma de análisis de dispositivos USB potencialmente peligrosos. La estrategia a seguir se apoya en el uso de un *sandbox* específico, desde el cual se realizarán las tareas de análisis de los dispositivos USB bajo estudio, sin peligro de afectar al equipo principal que se encargará de controlar las operaciones desarrolladas en el *sandbox* y de mostrar al usuario los resultados obtenidos en el análisis.

Respecto a la arquitectura y las tecnologías a emplear en la plataforma de análisis de dispositivos USB a desarrollar, se pretende hacer uso de lenguajes multiplataforma como Python o Java, de modo que la solución desarrollada sea utilizable en diversos entornos. La plataforma seguirá una arquitectura cliente-servidor, donde el servidor se ubicará dentro del *sandbox* y actuará como un contenedor de *plugins* de análisis, que serán los componentes responsables de las tareas concretas de análisis a realizar sobre los dispositivos USB bajo estudio.

Por otra parte, en lo que respecta al proceso de desarrollo a emplear, dado que los requisitos y detalles de la plataforma a desarrollar no están totalmente definidos en el momento de redactar esta propuesta, es recomendable plantear el uso de una metodología de desarrollo ágil como *Scrum*. Este tipo de metodología permite mitigar esta incertidumbre inicial, al contemplar en su propia organización del trabajo basada en iteraciones o *Sprints*, la gestión de requisitos cambiantes y la adición de nuevas funcionalidades a medida que el desarrollo avanza.