Atendiendo a las actividades que son realizables por parte del evaluador según el análisis en JIL, se propone a continuación un enunciado para simular un ejemplo de "juguete" (De ahí el nombre del enunciado) del cifrador CIFPECOM.

Enunciado del problema ("Toy Encryptor")

Entorno del problema

Se sabe que dentro del entorno del CIFPECOM existe un ordenador, el *"MC"*, con el que se puede acceder a funcionalidades de administrador del cifrador. Gracias a este ordenador es posible actualizar el firmware del cifrador o cargar sus claves de cifrado, entre otras cosas de relevancia para la seguridad del dispositivo. A este ordenador solo pueden acceder los managers que disponen de usuario y contraseña para su rol (O cualquiera que consigue vulnerar esas credenciales, por ahora imposible).

Las claves de cifrado que usará el dispositivo se cargan mediante una tarjeta Micro-SD y podrán ser utilizadas por los usuarios de rol *"Tropa"* con únicamente insertar la tarjeta que se les asigne en la misión. En esta tarjeta, a parte de la clave, la persona que utiliza el "MC" también carga las credenciales para que el rol "Tropa" pueda acceder, utilizar el dispositivo y comunicarse con sus compañeros de tropa de manera segura.

El cifrador funciona de manera simple. Cuando las tropas insertan la tarjeta, antes de cargar y hacer uso de la clave tiene que verificar que la persona que va a usar el dispositivo no es *"El malo"*, o de lo contrario podrían enterarse de todo lo que hablan y escriben las tropas y poner en peligro la misión.

Adicionalmente, el cifrador tiene un botón, el 'zeroizado', que permite a las tropas borrar de manera voluntaria toda información del dispositivo (Incluidas credenciales, claves…) y dejarlo en estado *"Inservible"* en caso de esta verse comprometida. En caso de que cualquier tropa se vea amenazada y piense que el enemigo podría acceder al dispositivo, siempre puede pulsar este botón y listo.

La función de verificación, en el caso de no poder verificar las credenciales en un máximo de 3 intentos, limpia los datos (como credenciales, claves u otra información que haya en el aparato), pero no lo deja inservible.

¡Nos atacan!

No todas las vulnerabilidades del sistema pasan por fallos software o hardware y, a veces, para poner en peligro la seguridad del sistema basta con haber dado acceso de la forma más tonta posible a quien no debíamos…

Siento dar la noticia, *"El Malo"* está entre nosotros. Alguien del equipo de administradores es un infiltrado y tiene credenciales para poder acceder al *"MC"* y cargar sus propias credenciales y claves en el cifrador, por lo que la información corre peligro.

Pueden darse dos casos en este problema:

- *"El Malo"* conoce credenciales de tropas auténticas y logra cargar su propia clave de cifrado.
    - *"El Malo"*, al haber cargado su propia clave, podrá descifrar fácilmente el mensaje, ya sea deshaciéndolo o por fuerza bruta.
- *"El Malo"* intenta cargar una clave mala, pero no conoce credenciales. Al autenticar, el sistema 'zeroiza' pero queda funcional y sin clave.
    - Acaba de descubrir un 'Exploit' del dispositivo que podrá aprovechar para ver la información de la comunicación "en crudo", sin cifrar. Además, este 'Exploit' ha hecho que el sistema limpie datos de auditoría y otros datos relevantes, por lo que se ha perdido información.

Nota: Este ataque supone y engloba que ha habido una mala programación *(Contiene Bad-Coding*), problemas por comportamientos lógicos (*No es así como se suponía que el 'zeroizado' debería funcionar),* errores por la gestión de credenciales (*"El Malo"* no debería tener ese acceso, fue un error humano dárselo), además de los problemas mencionados en el enunciado.