# Explicación del artículo "Strength of Two Data Encryption Standard Implementations under Timing Attacks" de Alejandro Hevia y Marcos Kiwi

## Integrantes

Azpeitia García Karyme — 317340385

Martínez Damaso Raúl Eduardo — 316155063

Pedro Méndez José Manuel — 315073120

Zamora Cruz Diego Arturo — 316249560

El artículo "Strength of Two Data Encryption Standard Implementations under Timing Attacks" de Alejandro Hevia y Marcos Kiwi analiza la vulnerabilidad de dos implementaciones del criptosistema Data Encryption Standard (DES) a los ataques de temporización.

Un ataque de sincronización es un método de criptoanálisis que explota el hecho de que los sistemas criptográficos suelen tardar cantidades de tiempo ligeramente diferentes en procesar distintas entradas. Esto puede utilizarse para obtener información sobre la clave secreta utilizada para cifrar datos.

En el artículo analizan dos implementaciones distintas de DES: una de software y otra de hardware.

En ambas implementaciones se muestra que el tiempo de ejecución de la varía en función del valor de la clave secreta. Esta variación en el tiempo de ejecución puede utilizarse para recuperar la clave secreta mediante un proceso de prueba y error, en la implementación de software pudieron recuperar la clave secreta tras 2.000 cifrados mientras que en la de hardware pudieron recuperar la clave secreta después de 10000 encriptaciones.

También se discuten varios métodos que pueden utilizarse para mitigar los efectos de los ataques temporales. Estos métodos incluyen:

- Usando una implementación en tiempo constante del criptosistema DES.

Una implementación en tiempo constante de un algoritmo criptográfico es donde se toma la misma cantidad de tiempo para procesar todas las entradas. Esto se puede lograr mediante el uso de una variedad de técnicas.

- Usando un acelerador de hardware criptográfico seguro.

Un acelerador de hardware criptográfico es una pieza de hardware específicamente diseñada para realizar operaciones criptográficas. Estos aceleradores están diseñados para ser resistentes a los ataques de sincronización.

- Usando un sistema operativo seguro.

Un sistema operativo seguro es uno que ha sido diseñado para proteger contra vulnerabilidades de seguridad, incluyendo ataques de sincronización. Estos sistemas operativos a menudo incluyen características tales como protección de memoria y aislamiento de procesos.

El artículo permite concluir que las implementaciones de software como de hardware del DES son vulnerables a los ataques de temporización y se recomiendan que los desarrolladores de implementaciones del DES tomen medidas para mitigar el riesgo de ataques de temporización, por ejemplo, utilizando contramedidas como implementaciones en tiempo constante.