¿Por qué no puedes clonar algunos mandos de garaje con un Flipper Zero?

Los mandos de garaje modernos suelen incorporar una tecnología denominada **Rolling Code** o **código evolutivo**.

La idea es sencilla: cada vez que pulsas el mando, **la señal transmitida cambia**.

Por ejemplo:

Pulsación 1 → Código A
Pulsación 2 → Código B
Pulsación 3 → Código C
Pulsación 4 → Código D

Por eso, aunque un dispositivo como **Flipper Zero** pueda detectar la frecuencia y registrar una transmisión de radio, **reproducir posteriormente esa misma señal no necesariamente abrirá el garaje**.

El receptor espera un código válido dentro de la secuencia prevista. Una grabación antigua puede haber quedado inutilizada después de utilizar el mando.

¿Qué diferencia hay con un mando de código fijo?

En un sistema de código fijo:

Mando → Código 1234
Mando → Código 1234
Mando → Código 1234

La transmisión puede ser siempre la misma.

Con Rolling Code:

Mando → Código A
Mando → Código B
Mando → Código C

La transmisión cambia continuamente.

¿Por qué se utiliza?

Principalmente para dificultar ataques de **repetición (replay attacks)**. Si alguien captura una transmisión, esa grabación no debería ser suficiente para reutilizarla posteriormente.

Esto es un buen ejemplo de cómo la **seguridad no depende únicamente de la frecuencia de radio**. Dos dispositivos pueden utilizar 433,92 MHz y tener mecanismos de seguridad completamente diferentes.

Conclusión: detectar una frecuencia no significa necesariamente que podamos clonar el mando. La frecuencia indica *dónde* se transmite la señal; el protocolo y el sistema de autenticación determinan *cómo* se valida.

#Ciberseguridad #IoT #FlipperZero #Radiofrecuencia #RollingCode #HackingÉtico #Seguridad