Antes de continuar leyendo esto quiero que quede terminantemente claro que clonar una tarjeta SIM puede ser ilegal en muchos países. Éste artículo está dirigido única y exclusivamente a los lectores interesados en informarse sobre como ayudar a aumentar la seguridad del sistema GSM, y no a romperla. El compartir la información de este artículo con lectores con intereses en la materia puede ayudar a que se descubran fallos que, luego de corregirlos, nos permitirá que todos disfrutemos de un sistema GSM más robusto.

Las tarjetas SIM tienen dos códigos secretos conocidos como **IMSI** (que sería algo así como el IMEI de los teléfonos) y **KI**. Éstos dos valores son enviados desde nuestro teléfono hasta el operador de telefonía móvil para que éste, previa comprobación de que esos valores efectivamente existen en su base de datos de clientes, pueda autenticarnos en la red GSM con nuestro número de móvil habitual.

El clonado de una tarjeta SIM consiste en obtener esos dos valores de la tarjeta a clonar y «programarlos» dentro de una tarjeta virgen, también conocida como Wafer. Posteriormente, esa tarjeta Wafer, nos permitirá autenticarnos en esa red como si fuera la original.
Obtener el IMSI es muy sencillo. De hecho, lo normal es que venga impreso en las mismas tarjetas SIM y que puedas leerlo si tienes buena vista, dado que es un número de entre 13 y 15 dígitos que está escrito con números muy pequeñitos. El KI, sin embargo, viene encriptado dentro del chip de la tarjeta y para obtenerlo es necesario realizarle un ataque de crackeo por fuerza bruta.

Pero antes hay que entender una cosa: al menos hasta la fecha de publicación de éste artículo existen tres tipos de tarjetas SIM basadas en tres tipos distintos de algoritmos:

- COMP128v1
- COMP128v2 (2004 y años posteriores, mejor recepción 3G, videollamadas, etc)
- COMP128v3.

Actualmente, sólo los chips que utilizan las versión 1 de esos algoritmos pueden ser clonados porque, al menos por ahora, es el único de los tres algoritmos que ha sido crackeado. Los proveedores de telefonía móvil han actualizado las tarjetas móviles de sus clientes con versiones posteriores al algoritmo 1, por lo que puede que la tarjeta que se quiera clonar ya no use el algoritmo crackeado. Si la tarjeta que se quiera clonar puede acceder a redes 3G y 4G modernas, es probable que ya no sea de las viejas. Sin embargo, hay muchos clientes que llevan muchos años sin actualizar sus SIMs, y puede que también sea el caso de la tarjeta en cuestión.
Pero, y como siempre digo, todo tiene un pero, los algoritmos v2 y posteriores agregaron protección física anti-manipulación y anti-copia a las SIM logrando que, al intentar leer la parte del chip que tiene el KI, esa porción de datos del chip se destruya, dejando inutilizada la tarjeta.
Para entenderlo más profundamente: La circuitería de la tarjeta SIM es como una computadora súper pequeñita. Tiene CPU, RAM, ROM, un espacio de almacenamiento escribible e incluso un SO que puede correr aplicaciones escritas para Java Card. Pero después de aplicarle esas medidas de seguridad v2 y posteriores, es una mini computadora que se blinda al momento de terminar de producirla, justo después de terminar de grabarle la KI en ese espacio de almacenamiento sólido. Y al estar blindada, no se puede acceder de la forma que se hacía con las tarjetas v1 sin riesgo de que salten los mecanismos de protección y destruyan el contenido de ese espacio de almacenamiento sólido.
Por eso hay que proceder con precaución. Con una tarjeta encriptada con el algoritmo v1 seguramente no habrá problemas. Pero para una SIM encriptada con algoritmo v2 o superior, lo mejor es trabajar con un software que haga una imagen de la tarjeta SIM y que te permita trabajar sobre esa imagen y no sobre la SIM real. Un ejemplo de un software así puede ser Dekart SIM explorer (700 dólares).