Llega la seguridad a los dispositivos móviles

Cada vez más se están utilizando los terminales móviles para actividades profesionales, además de las personales y esto ha hecho reaccionar a los fabricantes de móviles.

Las empresas y autónomos que utilizan dispositivos móviles para su trabajo diario, están preocupados por la seguridad de sus dispositivos, dándole un valor añadido, a la seguridad en estos dispositivos.

La respuesta de algunos fabricantes, no se ha hecho esperar y, ya disponemos en algunos modelos de gama alta, de la apreciada seguridad que demandan los usuarios.

En este caso hablaremos de uno de los fabricantes más conocidos, que en los dispositivos orientados al uso profesional, vienen protegido por "Samsung KNOX", también denominado Plataforma segura.

La plataforma de seguridad de Samsung KNOX se gestiona a través de tres protocolos: *Customizable Secure Boot*, *ARM® TrustZone®-based integrity Measurement Architecture* (TIMA) y un kernel con control de acceso SE for Android.

- **Customizable Secure Boot**
  Se trata de la primera línea de defensa del sistema, ya que bloquea el uso de todo software no verificado. Samsung KNOX *Secure Boot* puede ser activado de una forma sencilla en cualquier dispositivo ya adquirido. De este modo será posible reutilizar los dispositivos de uso personal para un entorno profesional reforzando la seguridad.

- **TrustZone-based Integrity Measurement Architecture**
  TIMA se encarga de proteger, controlar y verificar el estado de integridad del kernel. Cuando TIMA detecta que se ha violado la integridad del kernel o del gestor de arranque, ejecuta la política de seguridad pertinente, como por ejemplo deshabilitar el kernel y apagar el

dispositivo. ARM y TrustZone son marcas registradas de ARM Limited en la UE y otros países.

- **Android con seguridad reforzada** (SE Android)
  Permite separar aplicaciones y datos en diferentes dominios según su nivel de confidencialidad. *SE Android* aísla las aplicaciones y datos en diferentes dominios, reduciendo de esta forma el riesgo y los daños ocasionados por software malintencionado.

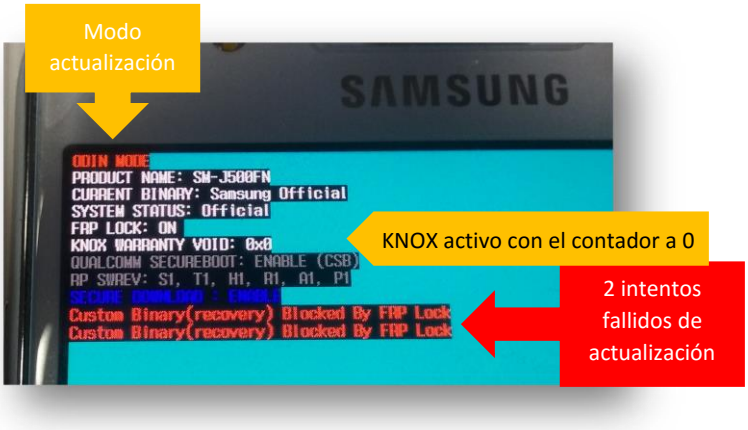
¿Es compatible la seguridad del terminal con aplicaciones de uso cotidiano como *WhatsApp*?

La respuesta sería sí, porque en este tipo de terminales, **no** se puede obtener la "key" del programa de mensajería "WhatsApp", para desencriptar la base de datos y manipularla.

No quiere decir que sea imposible descifrar la base de datos de "WhatsApp" sin la "Key", que en la actualidad está en "*.crypt8", lo dejaremos en muy complicado…

No obstante, en nuestra profesión, tenemos que tirar del sentido común y, si en un informe pericial, nos encontramos con un caso como este, aportando la siguiente prueba del terminal, podremos concluir de forma "probabilística" alta, que el terminal no ha sido manipulado.

Para comprobar este extremo se procedió, a encender un teléfono que lleva de origen instalado la plataforma segura, en modo "Downloading" y configurar los demás parámetros necesarios para proceder a una actualización del sistema operativo del terminal y, así poder actualizarlo, para poder entrar como **súper usuario**, utilizando para ello el software que manejan los ingenieros de Samsung "Odin3", el resultado se aprecia en la siguiente fotografía:



Esto garantiza que el terminal, **NO** ha sido manipulado, primero porque en el terminal se encuentra "Knox" tal y como indica el fabricante y por otro lado, sabemos que se mantiene su primera versión oficial, ya que el contador de "Knox" se encuentra a 0.

Con esto, tampoco se pretende afirmar que no se pueda actualizar o instalar una versión distinta de la original en el terminal, pero si nos encontramos con un terminal de este tipo y no lleva "Knox" porque ha sido actualizado, entonces podremos afirmar que el terminal, **SI** ha sido manipulado.

Creo que este paso en seguridad para los dispositivos móviles, es una tendencia que irán adoptando los distintos fabricantes para sus teléfonos de gama alta, orientados al uso profesional.