Investigadores:

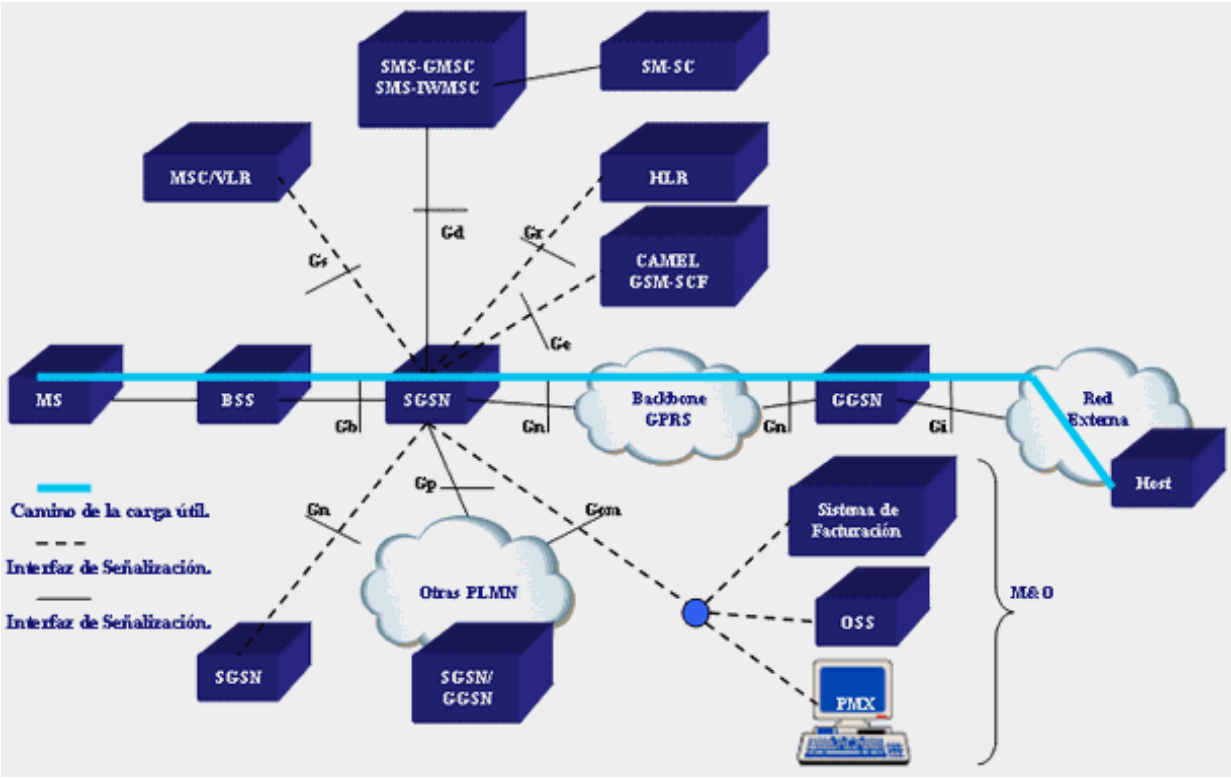
- Francisco Cortes (Chile)
- Manuel Moreno (Chile)

INTRODUCCIÓN

El siguiente documento describe y presenta un ataque práctico sobre equipos móviles (celulares) habilitados para usar las redes EDGE, GPRS, UMTS (en resumen, tecnología 2G y 3G). La intención es demostrar que es posible montar una BTS falsa (fake BTS), inducir a la "víctima" a conectarse a dicha BTS y ganar el control de las comunicaciones de datos de su teléfono. La posible ausencia de autenticación mutua en redes GPRS entre estación base y equipo de usuario, lo que hace vulnerable a GPRS frente al ataque de estación BTS falsa; segundo, la existencia del requerimiento de que los terminales móviles deben soportar el algoritmo de encriptación GEA0, hacen posible el ataque. Hay que hacer notar que el ataque de falsa BTS no depende de la debilidad del método de encriptación, por lo tanto es posible de realizar en casi toda ocasión.

Arquitectura GPRS/UMTS

Diagrama de una red celular cualquiera:



La estación de usuario (UE), nombre genérico que el mundo de las telco le da a los smartphones, notebooks con modem 2G/3G o a cualquier tablet con módulo 3G, establece una conexión con la BTS más cercana perteneciente a la PLMN de la cual el usuario es suscriptor.

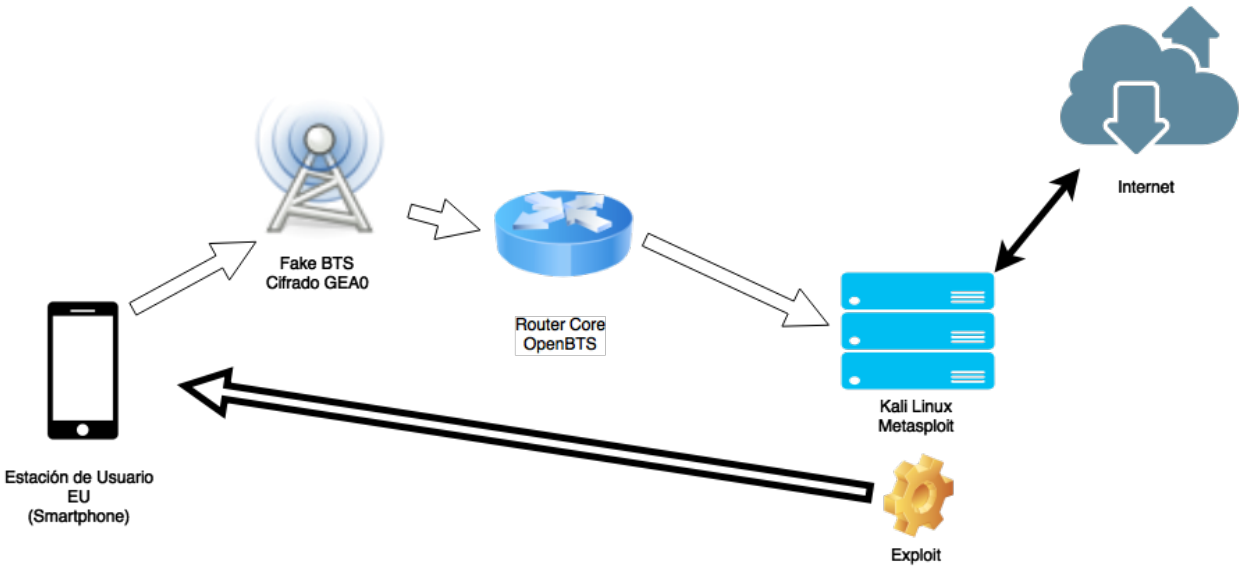
Luego de que el proceso de autenticación del usuario en la plataforma ha finalizado (aquí participa el MSC por el lado de voz y el SGSN por el lado de datos), se crea un túnel de datos IP entre el UE y el GGSN (Gateway GPRS Support Node), pasando a través de la BTS, el RNC (3G) o BSS (2G) y el SGSN (Serving GPRS Support Node). EL GGSN le asigna una IP al UE durante el proceso de creación de *"PDP (Packet Data Protocol) Context".* El UE envía los paquetes IP a través del túnel formado, donde los recibe el GGSN el cual esta encargado de rutear dichos paquetes hacia internet y de hacer el proceso inverso. Todos los paquetes van encapsulados usando protocolo GTP (GPRS Tunneling Protocol)

A nivel de aire y teóricamente, el uso de encriptación en la comunicación entre UE y Core es definido por la BTS. Durante los primeros mensajes, el UE le indica a la BTS los algoritmos de encriptación que soporta, y en base a eso ella decide qué algoritmo se usará y se lo hace saber al UE. La idea de nuestro proyecto es lograr setear el algoritmo GEA0 en el UE.

Respecto de lo anterior, podemos hablar un poco de las falencias teóricas que tiene el mundo GPRS:

- Falta de autenticación cruzada. El UE debe identificarse contra el Core a través de la BTS para poder utilizar sus recursos y obtener servicio, pero a su vez la BTS no necesita probar que es parte de la red Core a la cual pertenece el UE.
- Los terminales móviles, por defecto, deben soportar encriptación GEA0, la que en realidad no es ningún tipo o método de cifrado, solo es el nombre y norma.
- La necesidad de los terminales móviles de bajar de tecnología al existir degradación de la calidad de señal.

La falta de autenticación cruzada nos da el pie de entrada para desarrollar la primera parte de nuestro ataque: levantar un nodo con un dispositivo SDR y emular el Core Network usando el software OpenBTS con el fin de capturar el tráfico del usuario y darle acceso a una red controlada por nosotros para luego enviar un exploit al smartphone y tomar control total del teléfono, accediendo a la cámara, registro de llamados, sms enviados y recibidos, archivos del telefono, fotografías, videos, ubicación GPS actual y anteriores, conocer dispositivos alrededor de la víctima para lanzar futuros ataques a los otros dispositivos cercanos a nuestro objetivo.



Esquema del ataque.

Santiago de Chile, 20 de Julio de 2015