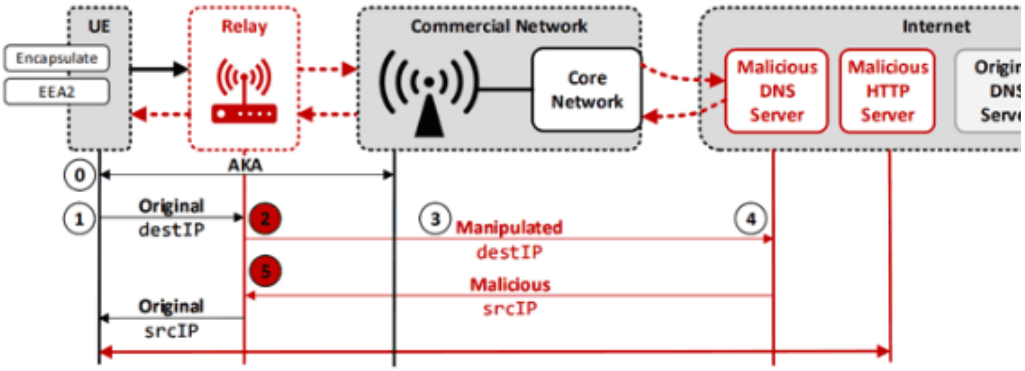
7) ¿Qué es un protocolo 4G?, ¿Para qué se usa?

El protocolo *Long Term Evolution* (*LTE*) más conocido como 4G es vulnerable a la interceptación y/o modificación de la comunicación de forma remota



ALTEr: Overview of the DNS redirection attack

Fuente: https://thehackernews.com/2018/06/4g-lte-network-hacking.html

Muchas compañías de comunicación implementan el protocolo *LTE* o, como se conoce normalmente, 4G, presente en la mayoría de dispositivos móviles. Las tecnologías provenientes de esta familia (3G, 4G, 5G) se gestan para proveer de mayor seguridad (entre otras cosas más) al antiguo protocolo GSM.
Un equipo de investigadores ha descubierto una vulnerabilidad en el protocolo que podría permitir a los atacantes espiar las comunicaciones que usan el mismo, pudiendo modificar el contenido e incluso redirigirlas a sitios web maliciosos.
Los investigadores han desarrollado tres nuevas técnicas contra esta tecnología que les permiten obtener la identidad de los usuarios, los sitos web visitados y redirigirlos a sitios web maliciosos a través de la suplantación DNS.

Podemos catalogar estas técnicas como «ataques pasivos» y «ataques activos». Interceptar la comunicación y la visualización de los sitios web visitados pertenecen a ataques pasivos. Por otro lado tenemos el ataque de suplantación de DNS conocido como ***«aLTEr»*** que permite a un atacante realizar un *«MiTM»* para interceptar las comunicaciones y redirigir a la víctima al sitio web malicioso utilizando *«DNS Spoofing»*.

La capa de enlace de datos de *LTE* está cifrada con AES-CTR, pero no está protegida su integridad, lo que permite a un atacante modificar los bits dentro de un paquete de datos cifrados. En los ataques LTE un atacante pretende emular una estación de comunicación real y así tomar el control de la comunicación. El ataque es muy peligroso pero difícil de explotar, ya que necesitamos hardware específico para ello, teniendo un alcance efectivo de casi 2 kilómetros

El futuro 5G

Las futuras redes 5G también se puede ver afectadas. Si bien es cierto que 5G admite el cifrado autenticado esta función no es obligatoria, lo que nos hace pensar que la mayoría de las compañías no tendrán intención de implementarla.

Para protegerse como usuario de estos ataques solo se ha recomendado usar *«HTTPS»*. El peso de la protección contra esta vulnerabilidad depende de las operadoras, que podrían solucionarlo actualizando su especificación de LTE (4G) para que use un protocolo de cifrado y autenticación como AES-GCM o ChaCha20-Poly1205. Sin embargo esto conlleva que las operadoras hagan un esfuerzo financiero y organizativo.