Honorables miembros de la Comisión de Transportes del Senado de Chile

En primer lugar, quisiera agradecerles la oportunidad que se me brinda de poder exponer sobre la seguridad de las plataformas que se están discutiendo dentro del marco de la ley que se está analizando. Mi exposición tratará principalmente sobre el hecho de que la geolocalización, es decir ubicación de una persona o un objeto vía GPS, es altamente inseguro si no se toman las medidas correspondientes.

Comenzaré esta exposición comentando sobre el "spoofing", técnica que permite simular posiciones GPS falsas. A través de esta técnica se puede hacer que un dispositivo que se encuentra en un sitio especifico muestre una posición diferente. Esto se logra a través del aprovechamiento de vulnerabilidades del sistema GPS que están presentes por décadas. No quisiera entrar en detalles técnicos, los que podrían ser parte de una exposición posterior, pero es obvio que la utilización de geolocalización vía GPS en plataformas, sin la adecuada protección, se presta para que ciberdelincuentes puedan realizar sus fechorías. Por ejemplo, en marzo de este año, en Suiza, en un evento de General Motors, se atacó el sistema GPS de vehículos Audi, Peugeot, Renault, Rolls Royce, Mercedes Benz y BMW. Se hizo creer que los vehículos estaban en Buckingham, Inglaterra, en el año 2036

Podemos fácilmente citar otros ejemplos de ataques que han aprovechado las vulnerabilidades de sistemas GPS no protegidos, donde encontramos secuestro de drones e interferencia en los sistemas de navegación de barcos, yate y camiones cisterna.

Con este tipo de ataques se intenta engañar a un receptor GPS mediante la retransmisión de una señal falsa desde la superficie que hace que todos los navegadores de las inmediaciones muestren una ubicación errónea. La suplantación de GPS se puede utilizar para secuestrar vehículos aéreos no tripulados (UAV por sus siglas en inglés) y coches o para confundir a taxistas, drones o marineros. Las herramientas necesarias para la suplantación de GPS son muy económicas, pues solo cuestan unos cientos de dólares. La tecnología contra la suplantación de GPS ya se está desarrollando, pero está destinada principalmente a sistemas más grandes, como la navegación marítima.

Hoy en día es extremadamente fácil falsear los datos de localización a través de aplicaciones gratuitas que se encuentran tanto para Android como para iOS. Dentro de la más comunes podemos citar:

1. Floater

Es muy sencilla de usar ya que tendremos un mapa sobreimpresionado en pantalla bastando desplazarlo hasta que el punto quede sobre la ubicación a simular. Podremos activar su funcionamiento o detenerlo directamente desde la barra de notificaciones e, incluso, planificar rutas ajustando la velocidad para que el móvil crea que se mueva.

Esta aplicación es gratuita y con publicidad, la que se puede eliminar a través de un pago de solo unos mil pesos.

2. Fake Location

Más sencilla que Floater, pero con lo necesario para la función que se desea: inventarnos una ubicación diferente de la real. Un mapa sobre el que arrastrar el punto de localización, un botón para que comience la simulación y listo. La aplicación engañará al móvil haciéndole creer que nos hemos teletransportado.

Esta aplicación es gratuita y con publicidad, la que se puede eliminar a través de un pago de solo unos mil pesos.

3. Fake GPS Location

Esta aplicación simula la posición de un móvil con sólo arrastrar el mapa hasta el lugar que quieras. Posee funciones adicionales tales como simular la geolocalización por WiFi, simular movimiento o calibrar manualmente la altitud. Esta aplicación es sumamente fácil de usar y es gratuita.

Yendo ahora a la temática que nos convoca, es decir la utilización de dispositivos móviles basados en GPS para su uso en el transporte de pasajeros podemos mencionar al menos dos problemas de seguridad que nos preocupan de sobre manera

1. Seguridad de las personas

El simple hecho de que la posición entregada por el GPS pueda ser falseada abre la posibilidad de que el pasajero que está utilizando el servicio de transporte público sea llevado a un lugar diferente al de su destino pudiendo ser asaltado o secuestrado, sin que su familia o cercanos sepan realmente donde se encuentra.

2. Tarificación

El hecho de que la posición pueda ser falseada abre la puerta a todo tipo de engaños sobre la tarifa a cobrar.

Frente a estos riesgos de seguridad es que planteamos que los dispositivos que serán usados por los servicios de transporte público sean seguros y que no permitan intervención alguna del sistema GPS que utilizan. Esto se logra a través del uso de plataformas que aíslan el sistema GPS de la aplicación que los está usando no permitiendo ninguna intervención maliciosa. Solo de esta forma podremos asegurar que las plataformas utilizadas pro los sistemas de transporte publico sean seguras y confiables.

Quedo a la disposición de esta comisión para profundizar o aclarar cualquiera de los puntos aquí presentados.