SEGUNDA PARTE. MARCO TEÓRICO

Marco Teórico del Campo de Acción

Luego de realizar un exhaustivo estudio y revisión bibliográfica sobre el tema, las conclusiones a las que pude llegar son las siguientes.

En muchos de los casos de equipos de rastreo satelital, como los Virloc por ejemplo, es posible implementar un password de 8 dígitos y utilizar un algoritmo de encriptación de los paquetes mediante Tiny Encryption Algorithm (TEA).

Los dispositivos se comunican a una dirección IP para transmitir sus datos. Allí se encuentra la base de datos que almacena y despliega en un mapa la información de los diferentes vehículos.

Muy bien, hasta aquí tenemos los dispositivos, los cuales a menos de tener acceso a los mismos es difícil de modificar.

Pero como en todo sistema, siempre hay un eslabón débil y en este caso se encuentra en el backoffice, lugar donde se almacena la información y se da acceso a los usuarios.

En general, el negocio de sistemas de monitoreo satelital está dividido en cuatro grupos de empresas, aquellas que fabrican los dispositivos de rastreo y control, las que desarrollan el software de gestión, las que proveen la geolocalización mediante mapas y por ultimo las empresas que instalan y proveen el servicio a terceros.

Es decir que compran un número de rastreadores, un sistema, accesorios y venden el servicio al público.

Estos sistemas se utilizan por dos motivos fundamentales:

- Protección de mercadería muy valiosa en tránsito (camiones de transporte)
- Protección de vehículos ante robos

Como podemos ver, están íntimamente ligados a la protección de activos valiosos, por lo tanto pueden ser objetivos de delincuentes "reales" no virtuales.

Haciendo un estudio "limitado" (revisión bibliográfica mencionada párrafos atrás) a un grupo del total de empresas que forman la cadena de valor de los productos de posicionamiento satelital, aparecen serias falencias que representan un riesgo para los usuarios de estos sistemas.

Equipos de rastreo

En lo que respecta a los equipos propiamente dichos, no tuve posibilidad de trabajar con ellos (exceptuando el caso del Virloc obviamente), la información que tengo está limitada al manual de operaciones de un equipo, por lo tanto no puedo emitir opinión sobre qué tan seguro es su sistema operativo o las medidas de seguridad física para su protección ante modificaciones.

Software Central de Seguimiento Satelital de vehículos

El software está dividido en una plataforma central, la cual se encuentra en las oficinas de las operadoras del servicio y un programa cliente.

El cliente puede ser web o una aplicación cliente/servidor.

Respecto al software que se ejecuta en el servidor, no tuve acceso directamente, por lo tanto tampoco puedo emitir opinión sobre del mismo en su totalidad. Hay ciertas pautas que muestran un diseño alejado de las buenas prácticas de seguridad.

En cambio sí pude acceder a clientes web de varios de estos servicios y bajé el programa cliente/servidor de una empresa que provee este software.

Veamos algunos problemas detectados y sus posibles consecuencias.

Las aplicaciones no utilizan ningún tipo de encriptación al comunicarse con el servidor, por lo tanto transmite los datos de usuarios y password en claro, con el consiguiente peligro de robo de cuentas y abuso por parte de terceros.

Los problemas no terminan aquí, ya que dentro de las aplicaciones hay errores más groseros y peligrosos para los clientes.

Los valores de los parámetros de las consultas se pasan por medio de GET, lo cual hace que puedan ser fácilmente modificables antes de ser enviados al servidor.

Si bien el envío por medio de un POST oculta estos parámetros, es insuficiente para detener a una persona con interés en conocer más allá de sus permisos.

En el caso de una de las aplicaciones que se encuentra en el mercado, una vez ingresado, se puede consultar los diferentes vehículos que conforman una flota.

Los parámetros enviados por la aplicación para consultar el recorrido de un vehículo, normalmente son los siguientes:

- vehiculoNombre
- vehiculo
- empr_id
- patente
- puerto
- usua_id

Donde "supongo" que los accesos están restringidos por flota y usuario. Es decir que un usuario de una empresa, debe poder ver solo los vehículos de su empresa.

Filtrando por los campos:

- usua_id
- empr_id
- vehiculo

Esto mostrara el recorrido o posición de un vehículo en particular.

El problema es que, si uno modifica el parámetro vehículo, el cual muchas veces es un número de cuatro dígitos, puede acceder a la posición de cualquier otro vehículo, independientemente de la flota o usuario. (Parameter tampering)

Modificando el parámetro vehículo podemos por acceder a transportes que no corresponden a la flota de la consulta.

Una de las consecuencias graves que trae el hecho de no incorporar encriptación entre el usuario y el server, es que un ataque de Man in the Middle puede modificar en tiempo real la ubicación de un transporte.

El vehículo, puede ser desviado del camino y quienes acceden al sistema pueden ver el recorrido normal (a menos que la empresa que tiene la custodia controle directamente desde el server la posición de los vehículos, pero como veremos más adelante esto tampoco es garantía de seguridad).

Cabe mencionar que también existen otros problemas que sufren estos sistemas como son SQL Injection, CRSF y XSS.

Empresas que realizan la instalación y gestionan el servicio de monitoreo

Aquí es donde está el talón de Aquiles de estos sistemas, las empresas que proveen estos servicios no tienen idea de lo que significa la seguridad informática, exponiendo a los usuarios a una falsa sensación de seguridad, dado que por malas implementaciones y vulnerabilidades en el software puede ser posible desde el acceso al equipo donde se gestiona la información, hasta ataques más sofisticados como el apagado de los vehículos en forma remota.

Problemas que detecté hay muchos, la mayoría de las empresas publicadas tiene una pobre infraestructura de seguridad informática, en algunos casos hasta se publican las empresas clientes. Información que debería ser confidencial.