11.1 Seguridad en Bluetooth

Bluetooth es la palabra que define un estándar global de comunicaciones inalámbricas para **redes de área personal** y que permite la transmisión de voz y de datos entre diferentes equipos por medio de un enlace por radiofrecuencia en entornos de comunicaciones móviles.

La tecnología Bluetooth tiene un alcance de unos **diez metros**, por lo que se ha integrado en dispositivos de la vida cotidiana que forman parte de las redes personales (PAN) como teléfonos y relojes inteligentes.

Los ciberatacantes que emplean estas comunicaciones suelen utilizar antes que amplían el campo de acción de la señal. Algunos de los ataques son los siguientes:

- **Bluejacking**. Consiste en el envío de spam al usuario por medio del intercambio con este de una vCard, de una nota o de un contacto.
- **Bluesnarfing**. Aprovecha las vulnerabilidades del protocolo para sustraer información del dispositivo atacado.
- **Bluebugging**. Utiliza técnicas de ingeniería social para que la victima acepte una conexión inicial para infectar el dispositivo con malware de control remoto.

A partir de ahí el usuario dispondrá de acceso remoto al teléfono del usuario y podrá utilizar sus funciones.

La adopción de algunas medidas de seguridad sencillas puede evitar los ataques. Por esta razón, deberían de formar parte de la conducta habitual de un usuario de dispositivos Bluetooh.

Algunas de ellas son:

- Activar bluetooh cuando sea necesario realizar algún tipo de comunicación a través de este medio y desactivarlo cuando se deje de utilizar.
- Cambiar el **nombre del dispositivo** para que no desvele datos personales y configurarlo para que permanezca oculto.
- No emparejar ni aceptar conexiones entrantes de **dispositivos desconocidos**, ya que la información podría estar infectada de software malicioso.
- Verificar periódicamente la lista de **dispositivos de confianza** para eliminar los que no se utilizan habitualmente.