SEGURIDAD EN EL INTERNET DE LAS COSAS

TRABAJO DE FIN DE GRADO

FRANCISCO MONTES GALLARDO

¿Qué es el Internet de las Cosas?

Tipos de dispositivos IoT

Dispositivos de uso comercial (IoT)

Esta categoria incluye la mayoría de los dispositivos que podemos encontrar en cualquier establecimeinto y que van a ser utilizados por usuarios finales. Ej. Cepillos de dientes, neveras o tostadoras inteligentes, wearables, etc.

Dispositivos de uso industrial (IIoT)

Por ser dispositivos para la industria, estos serán **más robustos y seguros** que cualquier dispositivo IoT comercial. Esto es lógico, puesto que la exigencia en una planta es enorme, debido por ejemplo a las altas temperaturas, corrosión o cualquier otro elemento de los dispositivos.

Usos del IoT

Transporte

Salud

Medio Ambiente

Agricultura

Vehículos Conectados

Industria Energética

Edificios Inteligentes

Farmacéutica

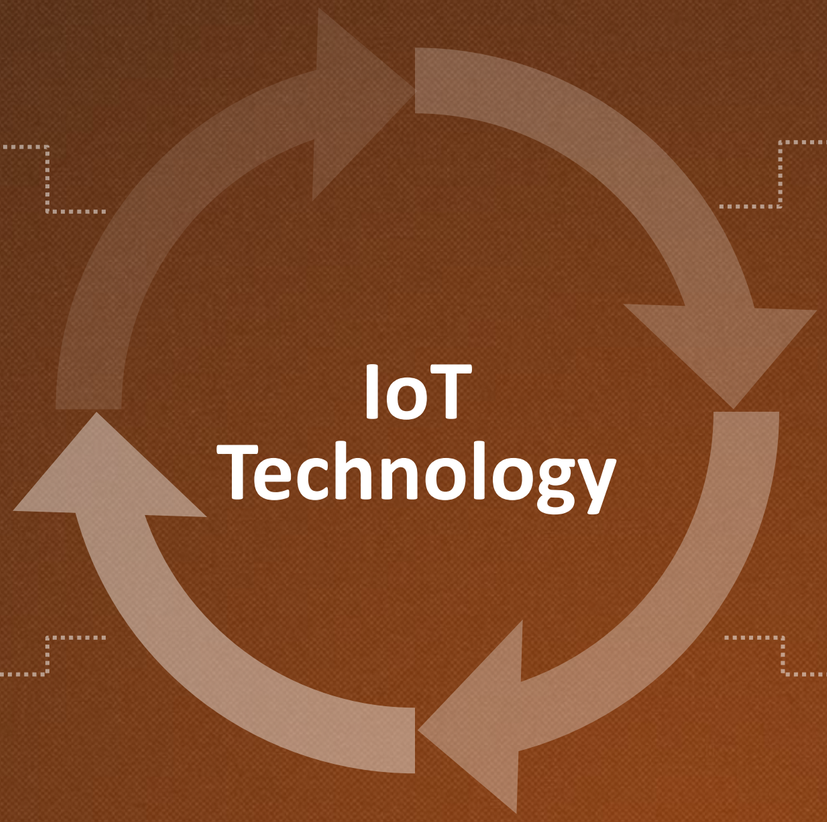
Tecnologías que utiliza el IoT

Sensores

Recopilan datos medibles de un IoT para después ejecutar una acción en base a esos datos

Servidor de Aplicaciones

Pueden ejecutar varios roles: ejecutar código de las aplicaciones, almacenar datos,autenticación de usuarios



Capa de Transporte

Redes inalámbricas; Bluetooth, ZigBee. Redes cableadas, IPv6

Protocolos; MQTT, TCP/IP,AMQP

Big Data

Ayudan a los analistas a comprender los datos analizados.

También tienen la capacidad de almacenar los datos y mantenerlos seguros

Seguridad IoT

Vectores de Ataque

IoT

Hardware

Seguridad a nivel físico del dispositivo IoT.

Se debe considerar por parte del fabricante este aspecto y asegurar la integridad y no permitir ningún tipo de manipulación directa.

Apps

Software

Aplicaciones que intentan mitigar los ataques a nivel de aplicaciones. Ejemplo MFA (Multi Factor authentication)

Sistemas operativos débiles e inseguros

Firewall

Red y transmisión

Todos los medios: Cable, satélites, inalámbricos son posibles de ser atacados.

Hay que proteger este nivel de seguridad en cuanto a la integridad, autenticación y encriptación.

Big Data

Cloud

SaaS – Software as a service

IaaS- Infra as a service

PaaS – Plataforma como servicio.

Users

Usuarios

Muchas de los problemas que pueden ocurrir en un ataque pueden empezar por el eslabón mas débil.

Ingeniería social y physing

Tipos de Ataques

Ataques físicos

Ataques de privacidad

Man in the middle

robo de información

Ataques DoS

control y uso malintencionado

Ataques de reconocimiento

SCADA

Ataques de acceso

Ataques a contraseña

Smart TV

Recomendaciones de seguridad

- Actualizar constantemente el firmware de la Smart TV y las aplicaciones que se ejecutan en el mismo
- Se prefiere las conexiones por cable a las inalámbricas
- Adquirir televisores inteligentes de proveedores acreditados
- Evitar conectar memorias USB al televisor porque pueden contener malware

Wearables

Vulnerabilidades

- Transmisión no segura de datos vía Bluetooth para el almacenamiento local del dispositivo
- Almacenamiento de datos inseguros en la nube
- Falta de autenticación y autorización
- Falta de controles de seguridad física
- Identidad del usuario y privacidad de datos
- Privacidad basada en la localización (GPS)

Connected Cars

Riesgos de seguridad

- Desbloquear y robar el coche
- Rastrear la ubicación
- Tomar el control de sus sistemas
- Hacerse con el control del GPS y guiar a un conductor a una ubicación no deseada
- Acceder a la información personal del conductor, incluido su nombre, correo electrónico, dirección del domicilio y datos bancarios (por ejemplo, número de tarjeta de crédito y fecha de caducidad)

Cámaras IP

Las cámaras IP se han convertido en un objetivo común para los atacantes

Recomendaciones de seguridad:

- Aplicar nuevos parches de seguridad
- Deshabilitar puertos o protocolos de red innecesarios
- Cambiar la contraseña predeterminada
- Implementar medidas de seguridad de red para descubrir o detener comunicaciones sospechosas.
- Asegurarse que se trata de una cámara IP segura

Futuro del IoT

El IoT es uno de los temas en auge de los últimos años, pero debemos ser totalmente responsables de las amenazas a los que estamos expuestos y poner fin a todas los que estén a nuestro alcance, al mismo tiempo en el que los fabricantes implanten las medidas de seguridad necesarias. De lo contrario, todo ello que a simple vista puede facilitarnos la vida nos la complicará por completo

Thank you!