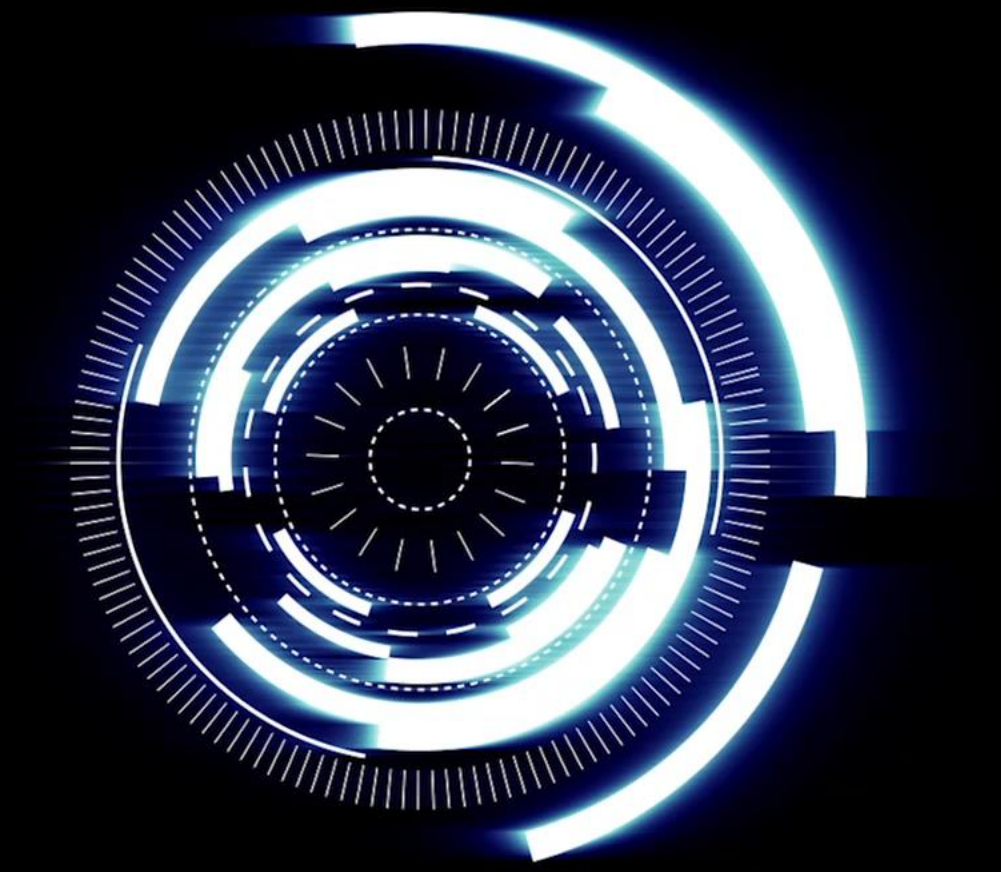
Deloitte.



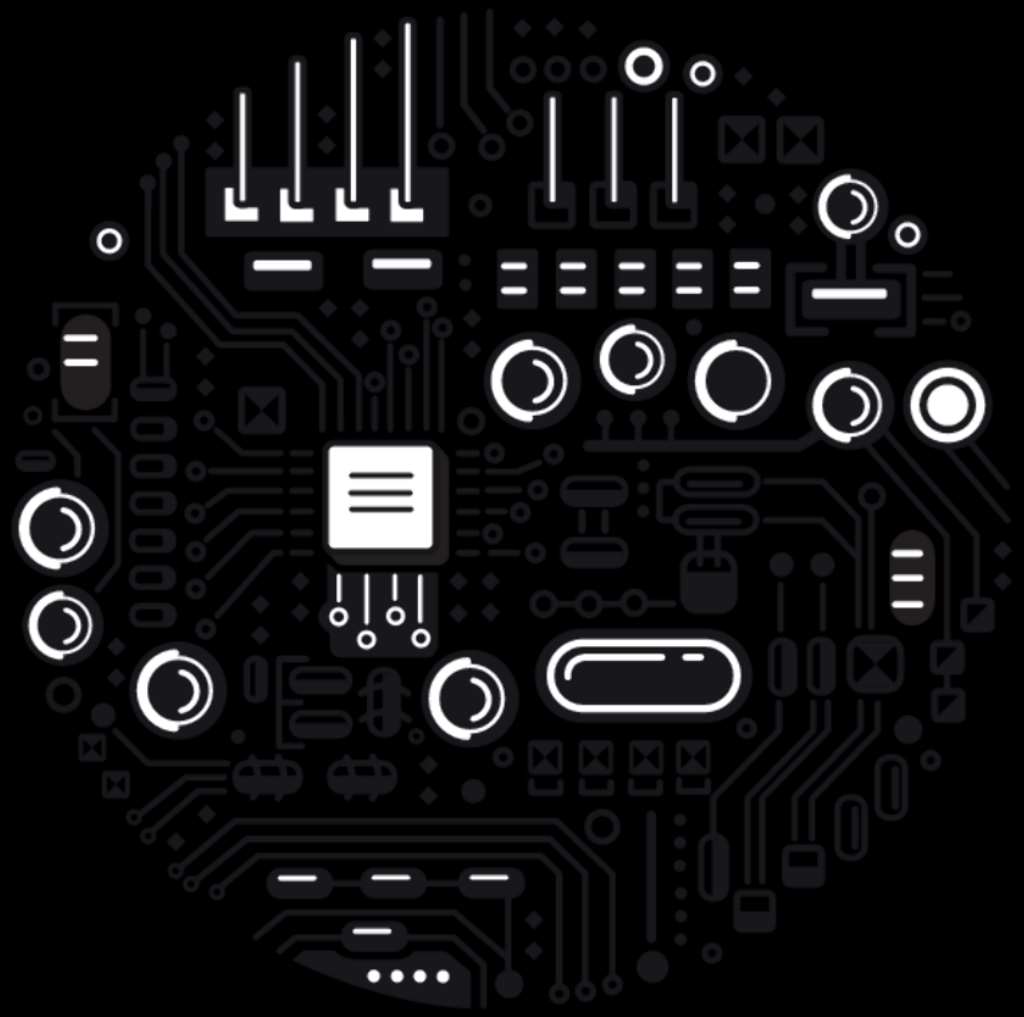
IoT

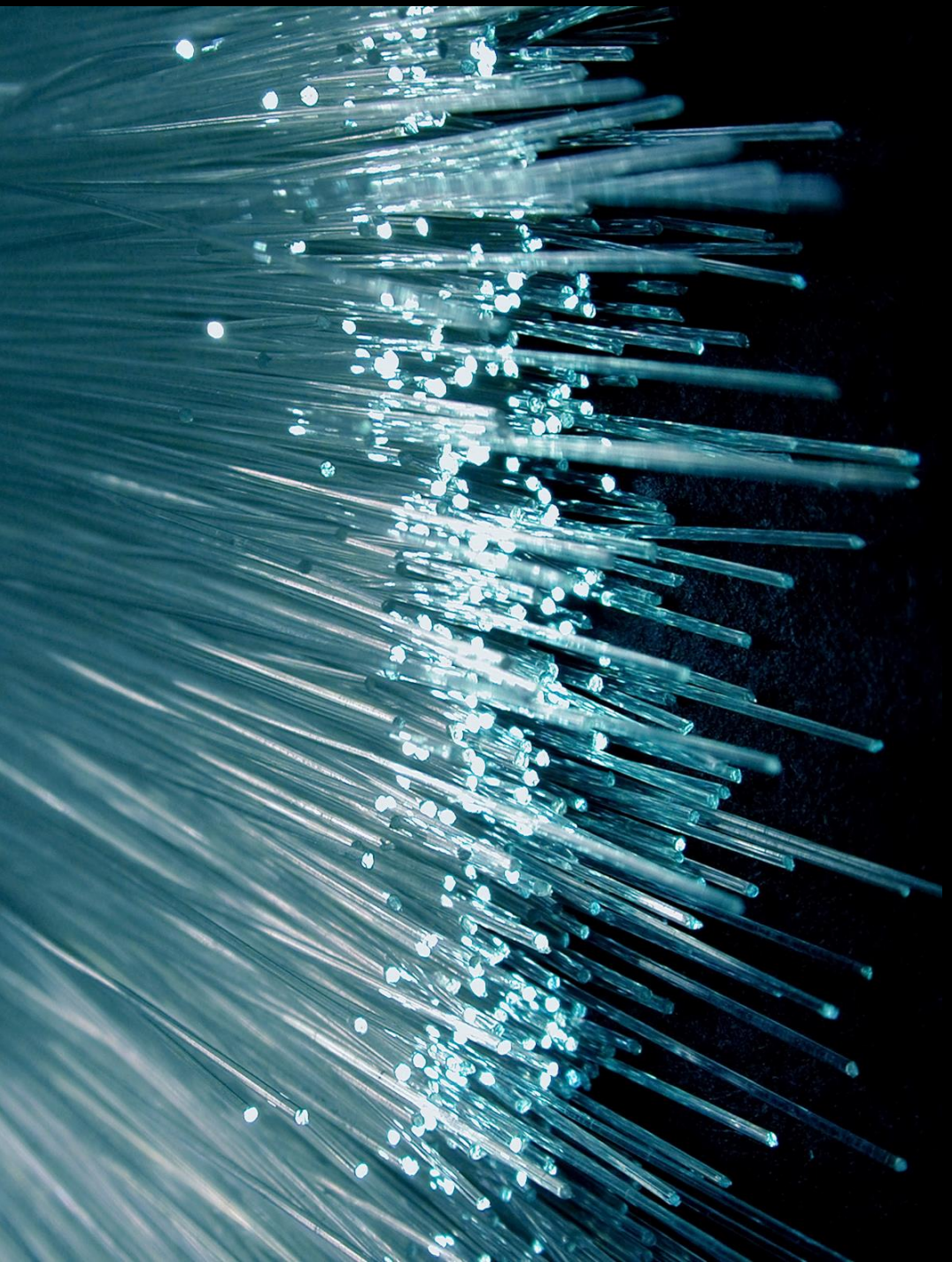
Seguridad en las Comunicaciones Inalámbricas

Alejandro Aliaga Casanova
Exp. Senior ERS IT

Agenda

- Contexto
- Nuevos Retos y amenazas
- Características de los dispositivos IoT
- ¿Conocemos y entendemos los dispositivos IoT?
- ¿Estamos preparados?
- Casos de Estudio
    - Smart Cities
    - Sistemas de control y telemetría
    - GSM
    - GPS
- Herramientas al alcance de un atacante
- Minimizando los riesgos
- Conclusiones





Contexto

"El internet de las cosas ya no es una tendencia, es una realidad. Hasta ahora la Humanidad nunca había vivido una revolución tecnológica de semejante magnitud como la que ahora mismo está teniendo lugar con el IoT"

Nuevos Retos
Nuevas Amenazas

Grupos pequeños, altamente cualificados, causan daños desproporcionados.

Motivaciones políticas, ideológicas o no esperadas puedes conllevar ataques dirigidos.

Aumento exponencial en la velocidad de amenazas, la ventana de respuesta se acorta.

Los ataques pueden ocurrir durante largos períodos de tiempo y de manera furtiva.

Impactos transversales, sin considerar el perímetro tradicional.

El ataque DDoS a Dyn solo ha sido el principio, los fabricantes deben asegurar los dispositivos IoT

Internet of Things believed to be targeted in massive DDoS attacks

Hackers used 'internet of things' devices to cause Friday's massive DDoS cyberattack

Características dispositivos IoT

- Dispositivos con poca capacidad de cómputo
- Escasa memoria
- Alimentados por Baterías
- Deben ser duraderos
- Deben disponer de comunicaciones inalámbricas
- Deben ser capaces de instalarse en cualquier parte de forma sencilla
- Deben tener una configuración sencilla o no tener configuración
- Precio reducido

¿Conocemos y entendemos los dispositivos IoT que nos rodean?

El 51% de los profesionales de ciberseguridad han sufrido ataques mediante dispositivos inalámbricos

Sólo el 31% de los encuestados tienen visibilidad de todos los dispositivos inalámbricos en sus redes.

El 89% de los encuestados no pueden monitorizar en tiempo real comunicaciones móviles (4G/LTE).

El 56% de los encuestados no pueden monitorizar todos los dispositivos IoT desplegados en su empresa.

Según un estudio de Gartner, en el año 2020 el 25% de los ataques serán protagonizados por dispositivos IoT

Solo el 1% de los encuestados aseguran estar completamente preparados para detectar amenazas vía dispositivos inalámbricos.

La mayoría de los profesionales de ciberseguridad no están preparados para la detección de ataques vía RF.

El 71% de los encuestados no pueden monitorizar otros protocolos inalámbricos que no sean Wifi.

El 70% de los dispositivos IoT no usan ningún sistema de cifrado en sus comunicaciones

Fuente:The Internet of Evil Things: Top Connected Device Threats in 2016

¿Estamos preparados para afrontar este nuevo reto?

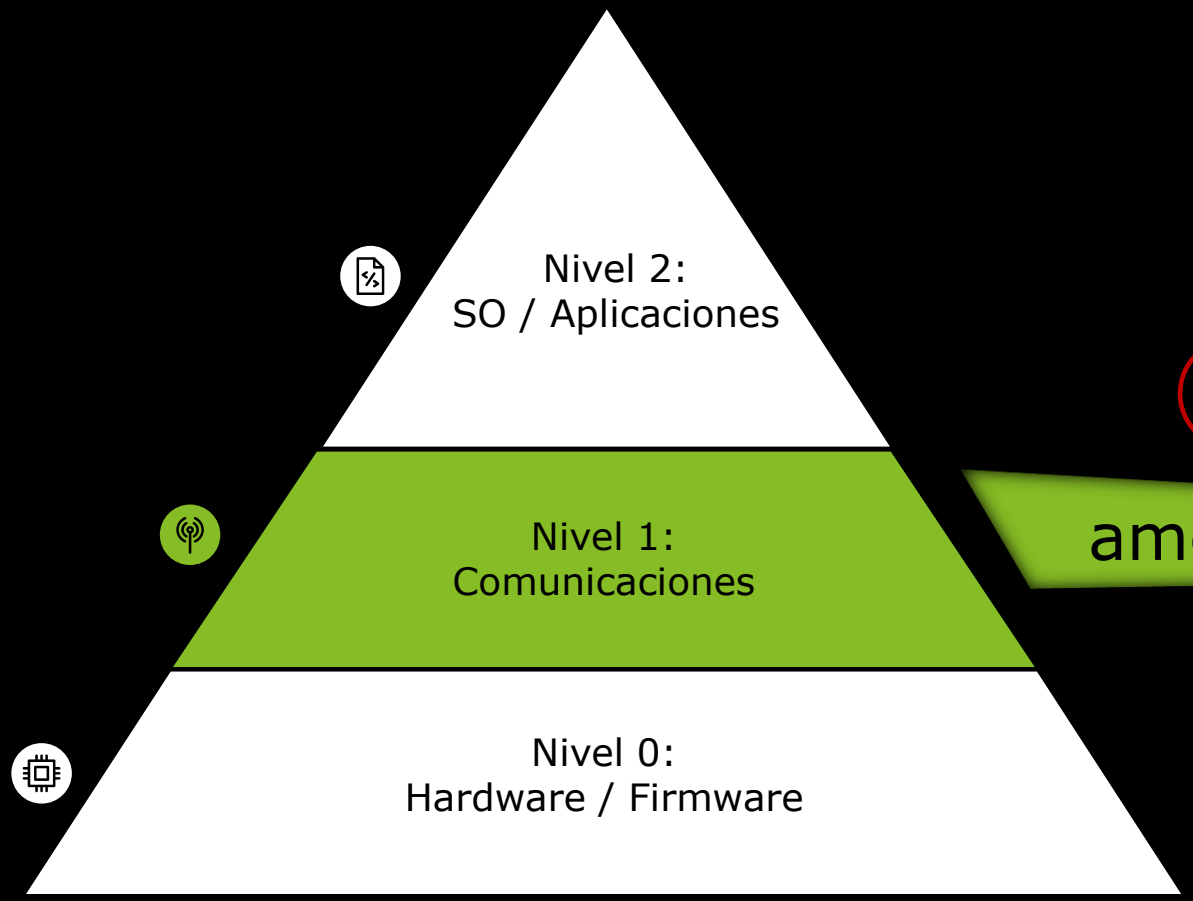
- Muchas soluciones de mercado se centran en defender el perímetro con soluciones que básicamente se centran en la seguridad IP, dejando de lado la seguridad de las comunicaciones inalámbricas.

- Cuando pensamos en securizar las comunicaciones inalámbricas pensamos en Wireless y Bluetooth dejando a un lado, otras tecnologías como: NFC, RFID, Z-Wave, LoRa, SIGFOX, Zigbee, TETRA, DMR, GSM, etc.

- Muchos dispositivos utilizan tecnologías inalámbricas mediante protocolos propietarios

- Actualmente muchos dispositivos están desplegados en las empresas, muchos de ellos desde hace años cuando, por definición, no se diseñaban pensando en la seguridad.

Estructura dispositivos IoT



amenazas

- Impersonificación
- Utilización de técnicas de Jamming
- Ataques Man in the Middle
- Integración de elementos fraudulento en la red
- Interceptación de comunicaciones
- Pérdida de confidencialidad
- Uso no autorizado de servicios
- Obtención de información
- Alteración de la información

¿Qué puede hacer un hombre con sólo una maleta?

Vectores de ataque, herramientas y consecuencias

Fuente:Pwnie Express – “Boston vs the Briefcase of D00M”

Casos de estudio

La seguridad de las comunicaciones en el mundo IoT

Casos de Estudio

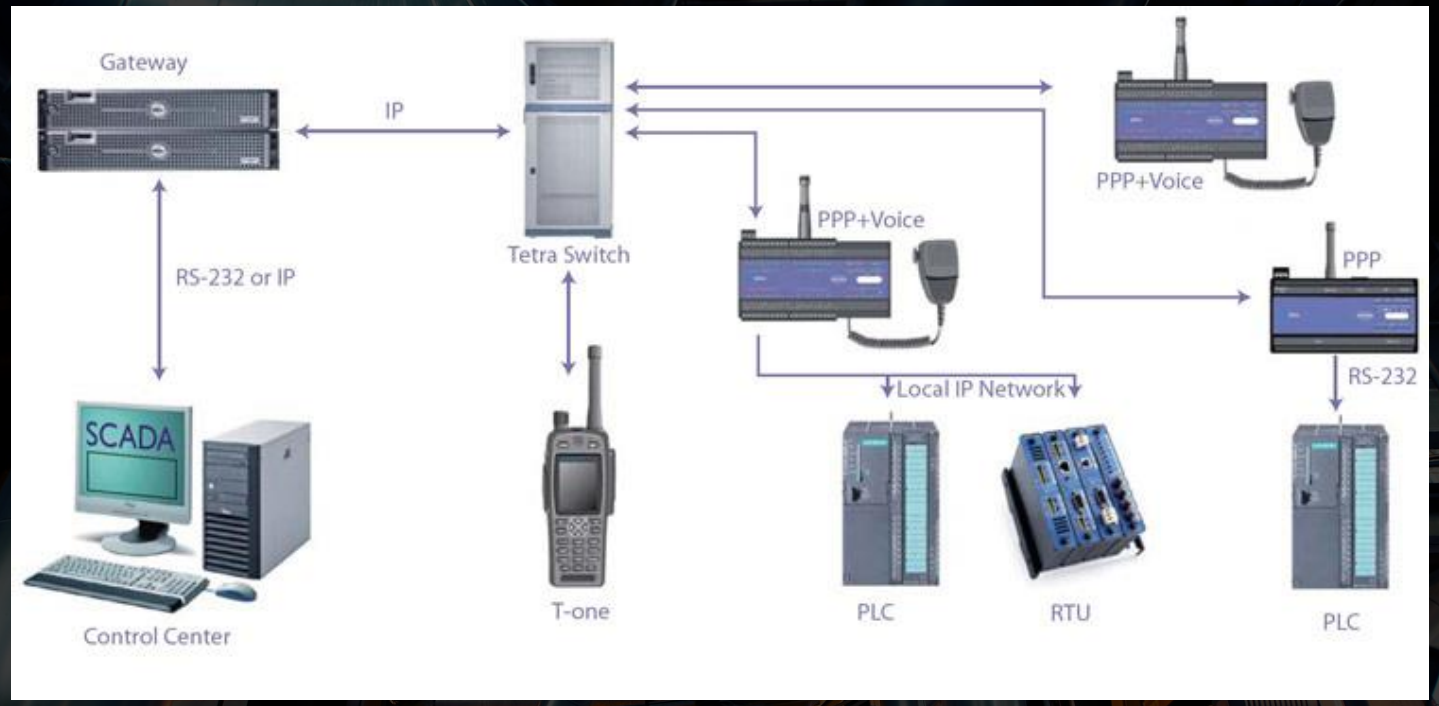
SmartCities

Con el crecimiento de las Smarticities se despliegan gran cantidad de dispositivos que, en la mayoría de los casos, se comunican de forma inalámbrica.

- Cámaras
- Semáforos
- Edificios
- Paneles de Mensajes
- Alumbrado
- Gestión Aguas

Estos dispositivos capaces de medir condiciones y extraer información deseada del lugar o del medio en el que se instalan se comunican con nodos que reciben esta información y la transmiten hacia un backend.

Casos de Estudio



alcanza un acuerdo con Motorola para mejorar el sistema automático de control de sus redes eléctricas

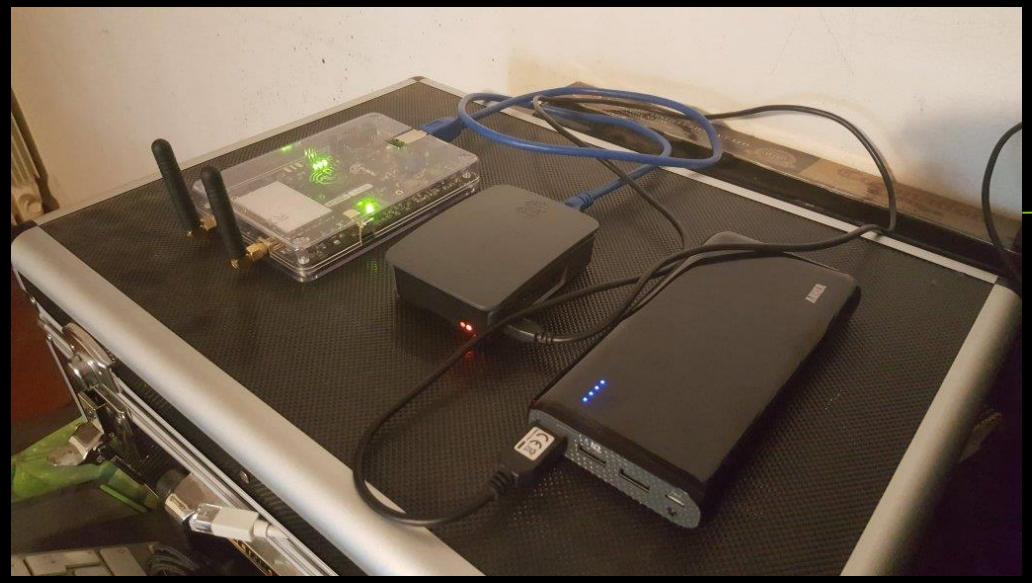
22/06/2007
Madrid

Sistemas de Control y telemetría

Los sistemas inalámbricos se están utilizando cada vez más en los sistemas de control y automatización industrial. La tendencia futura es conectar cada vez más dispositivos para proporcionar mayores capacidades.

Por su criticidad, la seguridad en los sistemas inalámbricos industriales debe abordarse en diferentes capas y requiere tanto la protección como mecanismos de detección temprana frente a ataques.

Casos de Estudio

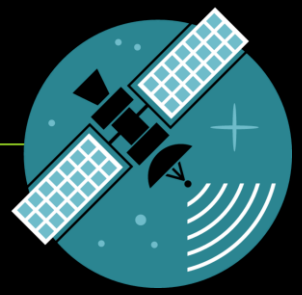


GSM / GPRS

Con un entorno correctamente configurado, un atacante con tan sólo un equipo SDR (radio definida por software) con un coste inferior a 400€, podría suplantar a un operador móvil legítimo, obligando a sus clientes a conectarse a su estación base para posteriormente:

- Interceptar las llamadas
- Interceptar los SMS
- Interceptar el tráfico GPRS
- etc.

Casos de Estudio



Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.

Ataques a las señales GPS

Mediante equipos SDR un atacante sería capaz de generar una señal GPS falsa (tiempo y posicionamiento).

- Empresas de logística (flotas)
- Ataques a certificados SSL (expiration date).
- Jamming
- Ataques a vehículos autónomos
- UAV / Aeronaves
- Muchos servidores NTP se basan en señales GPS
- Operaciones basadas en ventanas horarias (operaciones bancarias)
- Redes GSM/TDT que basan su modulación en base al tiempo GPS.

Casos de Estudio

Dispositivos médicos

'Medjacking' risk: Warning hackers could target wireless medical devices

J&J Warns Insulin Pump Vulnerable to Cyber Hacking

OneTouch Ping uses unencrypted radio signal

dyngnosis @dyngnosis · Sep 10

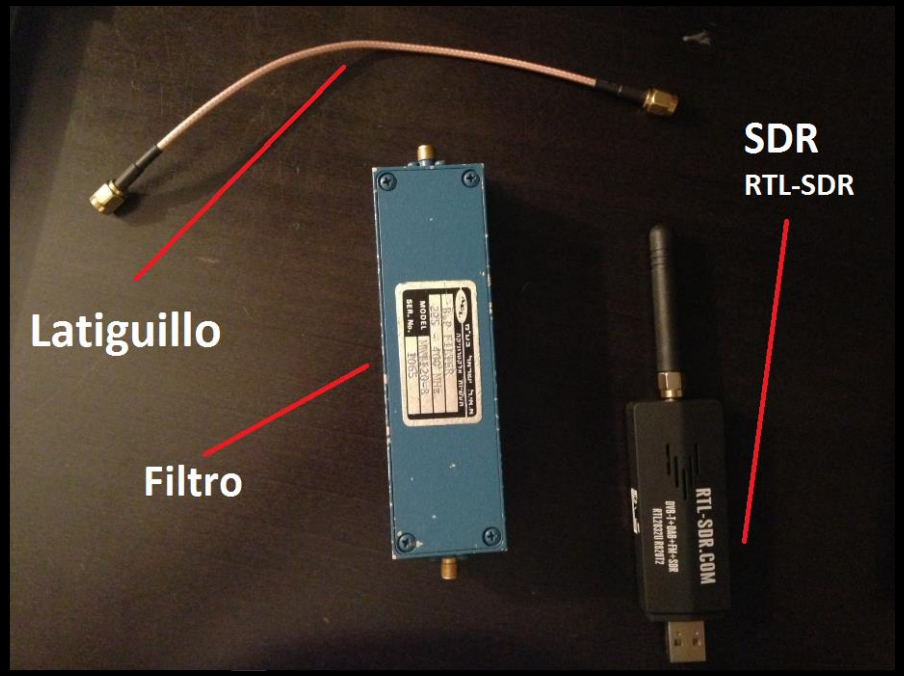
...MICS (Medical Implantable Communication Service) at 402–405 MHz. It uses a Reed-Solomon coding scheme together with CRC error detection..

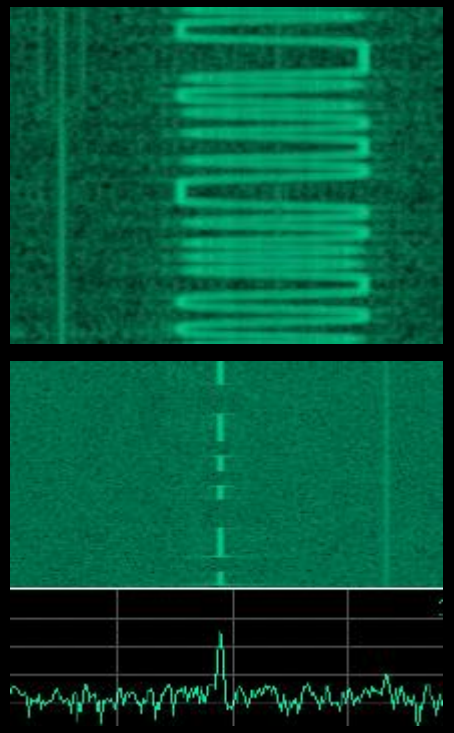
Los dispositivos se conectan usando tecnologías inalámbricas (402-405 Mhz) muy diversas y en muchas ocasiones no utilizan cifrado:

- Bluetooth
- Z-wave
- NFC
- Zigbee
- GSM
- Wifi

Estos dispositivos no son concebidos teniendo en cuenta la seguridad, son "cajas negras" con software propietario no sujeto a revisiones de seguridad.

Casos de Estudio





BladeRF

HackRF

USRP

Herramientas al alcance de cualquier atacante

Todos los ataques aquí mostrados se pueden realizar con equipamiento que puede estar al alcance de cualquier atacante con un presupuesto inferior a 1000€.

Estos equipos permiten generar señales de radio para realizar ataques de:

- Denegación de Servicio
- Jamming
- Suplantación de identidad
- Obtención de inteligencia a través de los datos obtenidos
- Etc.

Minimizando los riesgos

Un nuevo paradigma para la detección de ataques

Minimizando riesgos en RF

- Entender el nivel de exposición al riesgo
- Añadir a los procedimientos de seguridad un análisis del Espectro Radioeléctrico

- Mejorar la detección de dispositivos con comunicaciones inalámbricas mediante el despliegue de sensores.
- Monitorización continua de RF en busca de nuevas amenazas:
  - Rogue Devices
  - Network bridges
  - Insecure configs

- Mejorar las capacidades para la protección de ubicaciones de interés corporativo.
- Ampliar las capacidades de detección de transmisiones no autorizadas

- Integración del análisis del espectro radioeléctrico en sistemas de monitorización y alerta de la organización

Conclusiones

Seguridad de las comunicaciones inalámbricas en IoT

Conclusiones

- Debemos crear un nuevo enfoque en la seguridad de las comunicaciones.
- Es necesario crear normas y diseños que garanticen un diseño seguro.
- Las comunicaciones inalámbricas aumentan nuestra superficie de exposición.
- El riesgo para la privacidad de las comunicaciones ha aumentado considerablemente
- Facilidad para la realización de ataques activos y pasivos de interceptación.
- Abaratamiento de los costes del equipamiento HW
- La seguridad no debe basarse sólo a nivel IP, debemos monitorizar el espectro radioeléctrico.

Deloitte.