**Módulo 2**

Tema 1: Arquitectura IoT

RFID: identificación por radiofrecuencia: una de las primeras implementaciones de IoT.

EPC: código electrónico de producto. A diferencia del código de barras se pueden leer al mismo tiempo muchos productos, mucho más rápido y mejor acceso, etc. Administrados a nivel mundial por EPCglobal. ESTANDARES. UHF Gen2 / ISO 18000-6c

Sensores.

Las tarjetas RFID solían hacer mucho (leer, escribir, etc.) -> protocolos diversos.

Chips grandes, costosos, +energía.

Las tags pasivas particularmente obtienen energía del lector->+Cercanía->Menor nro. de apps.

Se decide poner solo el EPC -> etiquetas es in chip muy pequeño con antena imprimibles.

La información en la nube.

Hasta a nivel de producto.

Privacidad a tener en cuenta. Se agregaron otras cosas como aviso, etc. Por este motivo.

Prosperó por etiquetado a nivel artículo -> Industria de la ropa.

Pie para optimizar el inventario -> Crisis 2008

Arquitecturas a veces contra intuitivas como la de red eléctrica. Corriente alterna (Tesla). Incremento del voltaje para evitar pérdida de energía. CC (Edison) imposible a largas distancias.

Arquitectura celular. Dispositivos con celdas por antenas. Celdas entre celdas.

WWW:

Buenas arquitecturas

* No es continua. Metáfora de diseño simple.
* Interfaces estandarizadas.
* Modularidad – abstracción.
* Prevención de fallas en cascada.
* Reloj de arena. Estándares TCPIP, UDP hace que funciona cualquier cosa hacia arriba y hacia abajo. IP obviamente en el centro.
* Seguridad.
* Contra intuitiva.

IOT hoy. Telaraña de cosas. Código solo lectura imposible tocarlo. Todo lo opuesto a lo anteriormente planteado.

Cambiar las reglas demasiado dificultoso.

La idea es de subir todo a la nube y pensarla cada dispositivo físico como un avatar.

Problemas de tiempo real, por eso se implementan las versiones locales de la Nube->Fogs.

Tenemos distintos dispositivos, semánticas distintas, protocoles distintos, pero porque no pensar en cloud things y después interconectar todo en la nube.

Las interfaces de soft son mucho más fáciles de interconectar que las de hard.

Arena 3:

* Llevar las cosas a la nube.
* Loca proxy para realtime.
* Insertar las reglas en la abstracción de la nube.
* Firewall por encima de dicha atracción para poder exponer servicios.

**Si vamos a conectar 20 billones de cosas, mejor nos organizamos.**

**Marco antropológico es un buen marco. Organizar como POO.**

La nube es una buena metáfora de diseño… avatars.

Car structure: no es una línea directa al auto-teléfono sino a través de la nube. **Modelo que sigue TESLA.**

M2M: machine to machine es a través de la nube en realidad. MCM en realidad.

Tema 2: The web of thnigs

Una cierta manera IT es solo datos y otro no. Internet de las cosas son realmente los dispositivos.

Estandarización de los lenguajes, 2 niveles: internet of things y web. Web of things es una capa superior.

Datos públicos y privados. Acceso a cada una de ellas, seguridad, interrelación y alimenten a los sistemas.

La infraestructura subyacente será más heterogénea que lo ha sido para Internet.

No conectarnos sin ninguna seguridad sino más bien utilizando criptografía pública. Para cualquier cosa.

Diversidad: datos de diferentes puntos de vista. Bolsa de papas fritas.

Importancia de definir los estándares para cuando llegue la ola.

La importancia de enlazar dichos datos de tipos distintos. Hablar en mismo idioma.

Compatibilidad->Ver patrimonio neto.

IoT necesitará mucha interoperabilidad que no hay hoy. Necesidad de sistemas abiertos.

Internet: conjunto de protocolos TCPIP que conectan todas las computadoras.

La web, por encima de Internet, nivel más alto delos protocolos. Construcción de los lenguajes que van a ser necesario, formato de datos, para describir los distintos sistemas. Si se quiere es metadatos, datos de datos, nos permite realizar una descripción de todas las cosas.

Seguridad: por un lado del espectro datos públicos y por el otro, privados.

Es más importante para que se utilizan que el dato en sí.

No es solo censar sino controlar!!!

Tema 3: lecciones de Internet

Unos dicen que las cosas son muy débiles para ejecutar protocolos Internet y otras no. Primero se diseñaron para mainframe, luego pcs. La realidad que con las implementaciones se ejecutan bien en tablets, celulares, etc.

El debate no es si los dispositivos son débiles, sino si Internet es el marco adecuado para conectar cosas. Pensar en aplicar la forma de pensar de Internet y no los protocolos.

Metas:

* Restricciones que no restringen. Internet interfaz que justamente no restringe.

Reloj de arena: tecnologías por debajo de Internet y aplicaciones por encima. Capa simple en el medio TCPIP. Parte estrecha del medio porque hay menos diversidad.

* Interconexión heterogénea. 8 bits mismo orden.
* Alcance global -> Problema de seguridad. Es necesario en IoT?
* Generalidad: cualquier tipo de tráfico. Dispositivos generales o funciones fijas?

Defectos:

* Management: configuración, supervisión, diagnóstico a fallas. Fue muy difícil pensar en mover bits de un lado a otro. La administración de Internet es pobre, peor la adm. de apps.
* Seguridad: encriptar comunicación, restricción acceso, parche de vulnerabilidad. Aprender mirando aplicaciones y no internet.
* Movilidad: IP cuando se mueve cambia -> Reestablecer su identidad. Deberían haber separado la identidad de la ubicación.
* Longevidad: la info viaja con el nombre de dominio que cambia interfiere con nuestra capacidad de nombrar a largo plazo.

Tema 4: RFID

Ejemplos de IoT

* City lights.
* City IR Scan.
* Blood Scannng.
* Drones: mula de datos para recolectar datos donde es complicado acceder.

RFID tags activas: tienen baterías como el celular en cierto modo. Pasivas: sin batería.

Los protocolos de bajo nivel fueron implementados a partir de RFID tags pasivas para tener en cuenta todo el espectro y en bandas que puedan ser utilizadas en todo el mundo.

Este protocolo de etiquetas es como la capa física de datos.

El lector, además de comunicar, debe alimentar a las RFID tags.

Las RFID tags no se escuchan entre ellas (limitadas por capacidad) -> Necesidad de protocolo anticolisión.

EPC Gen2:

* Anticolisión.
* Selecciona. Se pude dirigir a un subconjunto (Clasifica). EPCGen2-01 Select.png
* Inventario. EPCGen2-02 Resto.png
* Acceso.

**FORO 2**

**El Internet de las Cosas 1**

Muy buenos comentarios, pienso que al tener que adoptar soluciones de software para implementar una arquitectura IoT, implica más que nunca, identificar los puntos vulnerables de la misma, analizar impacto ante posibles ataques y diseñar un esquema de seguridad acorde.

Por el lado cloud y con respecto a sistemas existentes, justamente hoy en día están bastante avanzados pero por mejorar, los mecanismos de seguridad. Pienso en apps basadas en fitbit intercambiando datos vía oauth <https://dev.fitbit.com/build/reference/web-api/oauth2/>

Por el lado fog, me sentí identificado con el comentario de @jorge gomez stechina con respecto a que lo veía más como una intranet, inclusive formando una DMZ, pero también considero válido lo que menciona @maimiliano Alberto cucchetti que es más bien una categorización, aunque dicha infraestructra fog debería responder a requerimientos de tiempo real, etc.

Este tema fog y la seguridad implementada en la cercanía de los dispositivos es donde estoy tratando de asimilar aún y me gustaría avanzar con una arquitectura concreta de bajo nivel, por ejemplo, para una casa inteligente.

Saludos a todos.