

/Root@d° 2016

La cena de los idloTas

Internet of Things (IoT)



www.dinosec.com

@dinosec

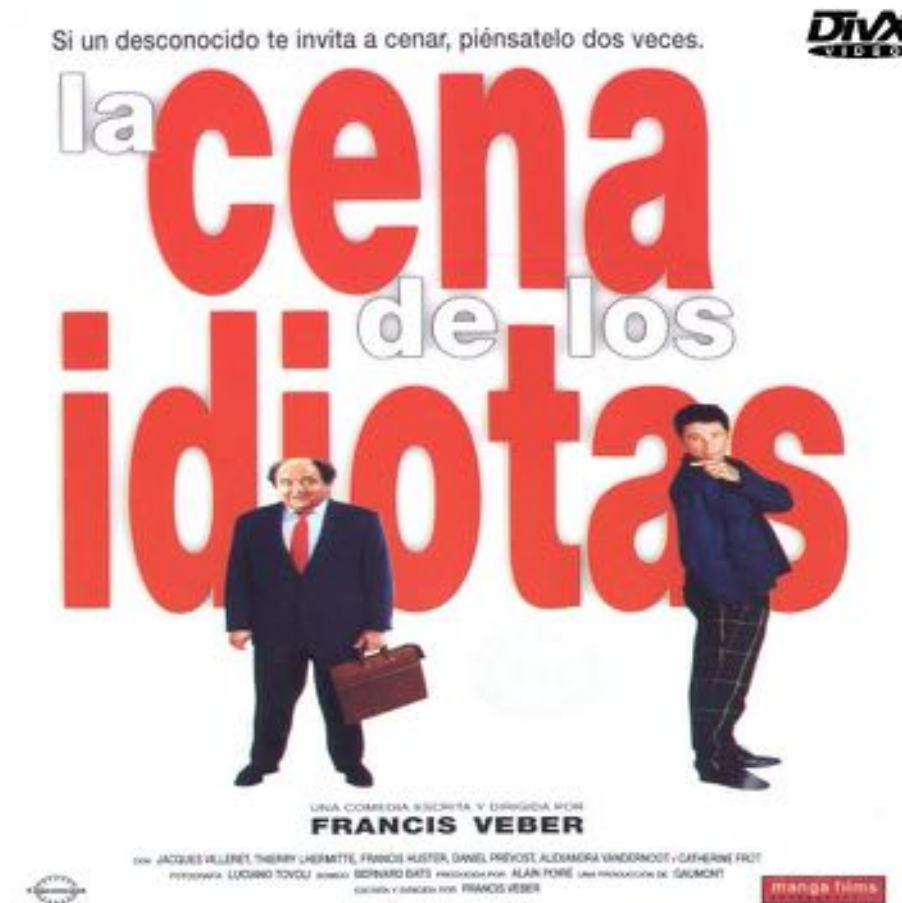
Raúl Siles

raul@dinosec.com

@raulsiles, @dinosec

March 5, 2016

La cena de los idloTas



La cena de los idloTas

- "Pedro Herrando celebra cada miércoles con sus amigos, todos ellos importantes hombres de negocios, lo que ellos denominan "la cena de los idloTas", un encuentro en el que cada uno de los asistentes debe ir acompañado de un 'personaje bizarro o esperpéntico', del que todos puedan reírse. Cada 'invitado' tiene su propia personalidad, historias, debilidades y peculiares comportamientos. Aquél que haya presentado al 'invitado' más idloTa de la cena, recibe el reconocimiento de sus compañeros al final de la velada."

La cena de los idloTas

- "Pedro Herrando celebra cada miércoles con sus amigos, todos ellos importantes hombres de negocios, lo que ellos denominan "la cena de los idloTas", un encuentro en el que cada uno de los asistentes debe ir acompañado de un 'personaje bizarro o esperpéntico', del que todos puedan reírse. Cada 'invitado' tiene su propia personalidad, historias, debilidades y peculiares comportamientos. Aquél que haya presentado al 'invitado' más idloTa de la cena, recibe el reconocimiento de sus compañeros al final de la velada."

La cena de los idloTas

- "Pedro Herrando celebra cada miércoles con sus amigos, todos ellos importantes hombres de negocios, lo que ellos denominan "la cena de los idloTas", un encuentro en el que cada uno de los asistentes debe ir acompañado de un 'artilugio bizarro o esperpéntico', del que todos puedan reírse. Cada 'dispositivo' tiene su propia personalidad, historias, debilidades y tecnologías inalámbricas. Aquél que haya presentado al 'dispositivo' más idloTa de la cena, recibe el **reconocimiento** de sus compañeros al final de la velada."

IoT o IoE



- Internet of Things (IoT)
 - Cisco: 12,5 b (2010), 25 b (2015), 50 b (2020)...
 - 2014: 10 'cuatrillones' de hormigas (10.000.000.000.000.000)
 - Gartner: 26b (2020)
 - IDC: 212 b (2020)
 - 7,7 billion people (2020) ($\approx \times 30$)

BILLIONS
&
BILLIONS



- Internet of Everything (IoE)
 - Sustantivo: Cosas, animales y ...
personas



¿Seguro que es seguro el IoT?

- Termostatos Heatmister
 - Acceso remoto a servicios (puertos TCP), credenciales por defecto, vulnerabilidades web, contraseña Wi-Fi en claro, ¿actualizaciones?...
- Bombillas inteligentes LIFX - ¿actualizar?
 - Contraseña Wi-Fi vía 802.15.4 6LoWPAN (¿cifrado?)
- Bombillas inteligentes Philips HUE
 - Bridge / controller ZigBee Light Link (ZLL) – token de autenticación basado en MAC (apagón)
- Alarma SimpliSafe
 - Comunicación bidireccional no cifrada (PIN)
 - Estación base, teclado y multitud de sensores
 - ¿Actualizaciones? ROM
 - OOK (315/433 MHz)



Referencias

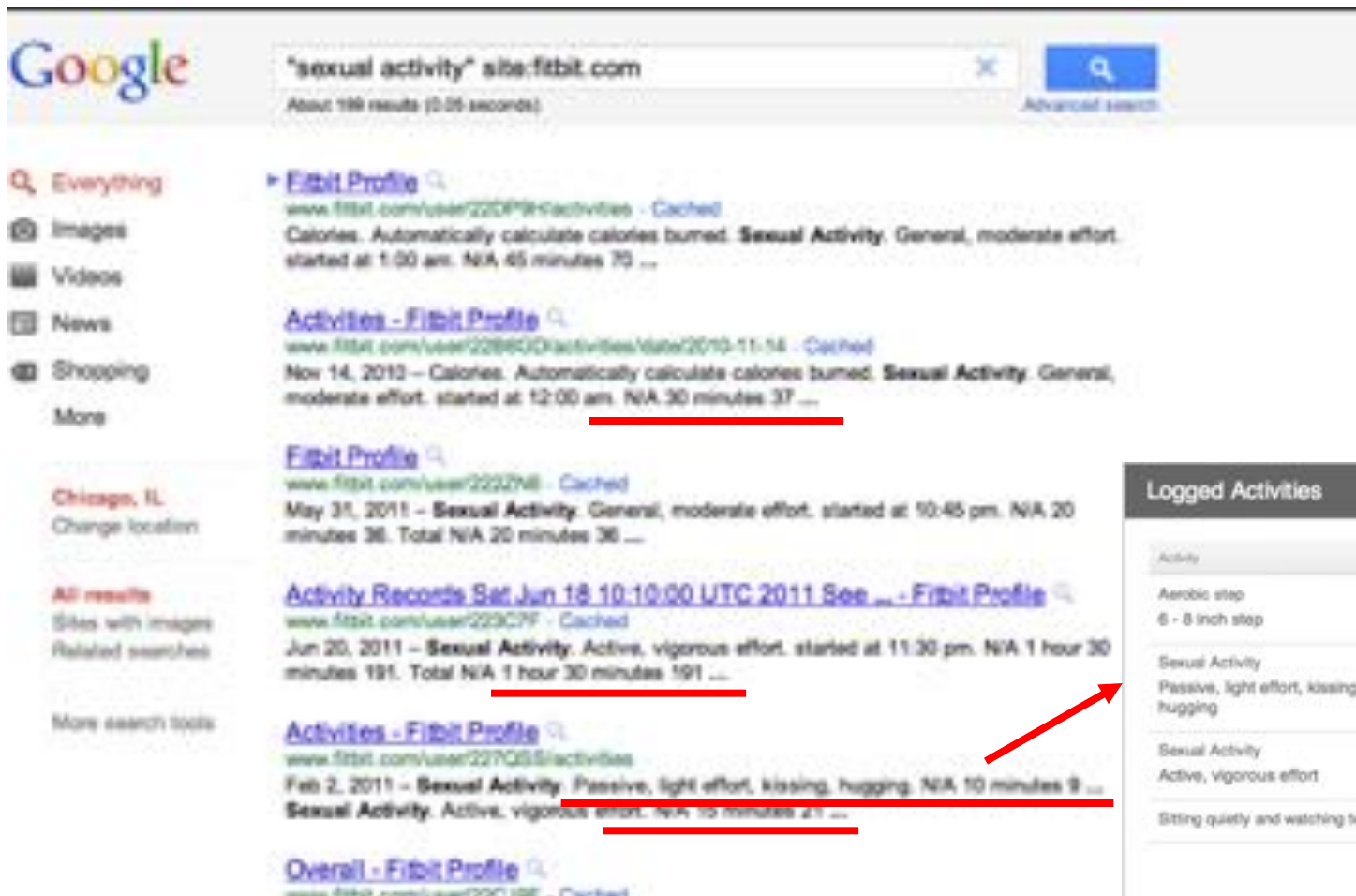
- <http://cybergibbons.com/security-2/heatmiser-wifi-thermostat-vulnerabilities/>
- <http://contextis.com/resources/blog/hacking-internet-connected-light-bulbs/>
- <http://www.dhanjani.com/blog/2013/08/hacking-lightbulbs.html>
- <http://blog.ioactive.com/2016/02/remotely-disabling-wireless-burglar.html>

“Hacer ejercicio es saludable...”

- Pulseras y apps deportivas y de salud
 - ¿Para profesionales o para vida saludable?
 - Localización, distancia, velocidad, calorías consumidas, ritmo cardiaco, evolución, etc
 - Datos físicos personales y... anuncios
 - Apps gratuitas
 - “Si no estás pagando, tú eres el producto”
 - Redes sociales y publicación de actividades
 - Movimientos (Apple Healthkit y Google Fit)
 - ¿conduces, vas en bici, andas, corres, duermes...?
 - M8: Estimar distancias y elevación (barómetro)
 - Contador de pasos vs. ir en bici (¿distancia?) vs. subir escaleras



“...y la actividad sexual también...”



Google search results for "sexual activity" site:fitbit.com. The search bar shows the query and the number of results (About 188 results (0.05 seconds)). The results list several Fitbit profiles with sexual activity logs. A red arrow points from the search results to the "Logged Activities" table on the right.

Search results include:

- Fitbit Profile** - www.fitbit.com/user/220P9H - Cached. Calories. Automatically calculate calories burned. Sexual Activity. General, moderate effort. started at 1:00 am. N/A, 45 minutes 70 ...
- Activities - Fitbit Profile** - www.fitbit.com/user/2284C3C/activities/date/2010-11-14 - Cached. Nov 14, 2010 - Calories. Automatically calculate calories burned. Sexual Activity. General, moderate effort. started at 12:00 am. N/A, 30 minutes 37 ...
- Fitbit Profile** - www.fitbit.com/user/22227N6 - Cached. May 31, 2011 - Sexual Activity. General, moderate effort. started at 10:45 pm. N/A, 20 minutes 36. Total N/A, 20 minutes 36 ...
- Activity Records Sat Jun 18 10:10:00 UTC 2011 See ... - Fitbit Profile** - www.fitbit.com/user/223C7F - Cached. Jun 20, 2011 - Sexual Activity. Active, vigorous effort. started at 11:30 pm. N/A 1 hour 30 minutes 191. Total N/A 1 hour 30 minutes 191 ...
- Activities - Fitbit Profile** - www.fitbit.com/user/227C5S/activities. Feb 2, 2011 - Sexual Activity. Passive, light effort, kissing, hugging. N/A 10 minutes 9 ... Sexual Activity. Active, vigorous effort. N/A 10 minutes 21 ...
- Overall - Fitbit Profile** - www.fitbit.com/user/22C13E - Cached.



Logged Activities				
Activity	Distance	Duration	Cal	Fat
Aerobic step 6 - 8 inch step	N/A	45 minutes	355	☆
Sexual Activity Passive, light effort, kissing, hugging	N/A	10 minutes	9	☆
Sexual Activity Active, vigorous effort	N/A	15 minutes	21	☆
Sitting quietly and watching television	N/A	1 hour	56	☆
Total	N/A	2 hours 10 minutes	441	

<http://techcrunch.com/2011/07/03/sexual-activity-tracked-by-fitbit-shows-up-in-google-search-results/>

“¡Pero con moderación!” 😊



Jeff
Male
Joined Dec 9, 2010

Privacy Settings

Public Search Engines:
☒ Allow my profile to be found in search results (Google, Bing, etc)

Jeff has not uploaded any pictures

OverallFoodActivitiesWeightJournal

Logged Activities

Fri, Dec 10

Activity	Distance	Duration	Calories	Rate
Sexual Activity Active, vigorous effort started at 2:00 pm	N/A	<u>4 hours 15 minutes</u>	347	
Total	N/A	4 hours 15 minutes	347	

IoT

- Internet of Things
- Internet of Toys
- Internet of 'Tontos'

vtech



Ámbitos del IoT...

- *Smart Cities and Critical Infrastructures*
 - Sensores de seguimiento de transporte público, iluminación pública, calidad del aire y del agua, plazas de aparcamiento, cámaras, distribución eléctrica, semáforos, 'aglomeraciones', parques/jardines y plantaciones, turismo, marquesinas, localización de tu vehículo, etc.
 - Infraestructuras críticas, control industrial, SCADA, etc.
- *Personal, Smart Homes, and Smart Offices/Buildings*
 - Pulseras deportivas, relojes, móviles, enchufes, bombillas, beacons (geo-fencing), cámaras, alarmas, consumo eléctrico, climatización, temperatura, humedad, estaciones meteorológicas, detectores de humos, caldera, luminosidad, movimiento, sensores magnéticos, inundación, persianas, accesos (garajes), mandos de apertura remota, cerrojos, timbres, electrodomésticos y TV, vehículos, gafas, juguetes, dispositivos médicos, etc.

La seguridad del IoT... tiene güevos



Seguridad del IoT

- Análisis de firmware
 - ¿Protecciones (modernas) anti-exploiting?
 - Servicios legendarios (¿telnet?)
 - Contraseñas y datos sensibles ¿cifrados?
- Interfaz de administración web
 - Desplazamiento por directorios, LFI/RFI, XSS, CSRF, autenticación, control de acceso, gestión de sesiones, etc.
- Aplicación móvil de gestión
- Integración en la nube
- Tráfico de red ¿cifrado?
- **Comunicaciones inalámbricas**

PWRH Training Bootcamp

Nueva edición en
#rooted2017

/Rooted[®]CON



www.dinosec.com
[@dinosec](mailto:raul@dinosec.com)

PWRH

Practical Wireless & Radio Hacking



Raúl Siles
raul@dinosec.com
[@raulsiles](https://twitter.com/raulsiles)

March 1-2, 2016 – RootedCon 2016

2016 © Dino Security S.L.
All rights reserved. Todos los derechos reservados.

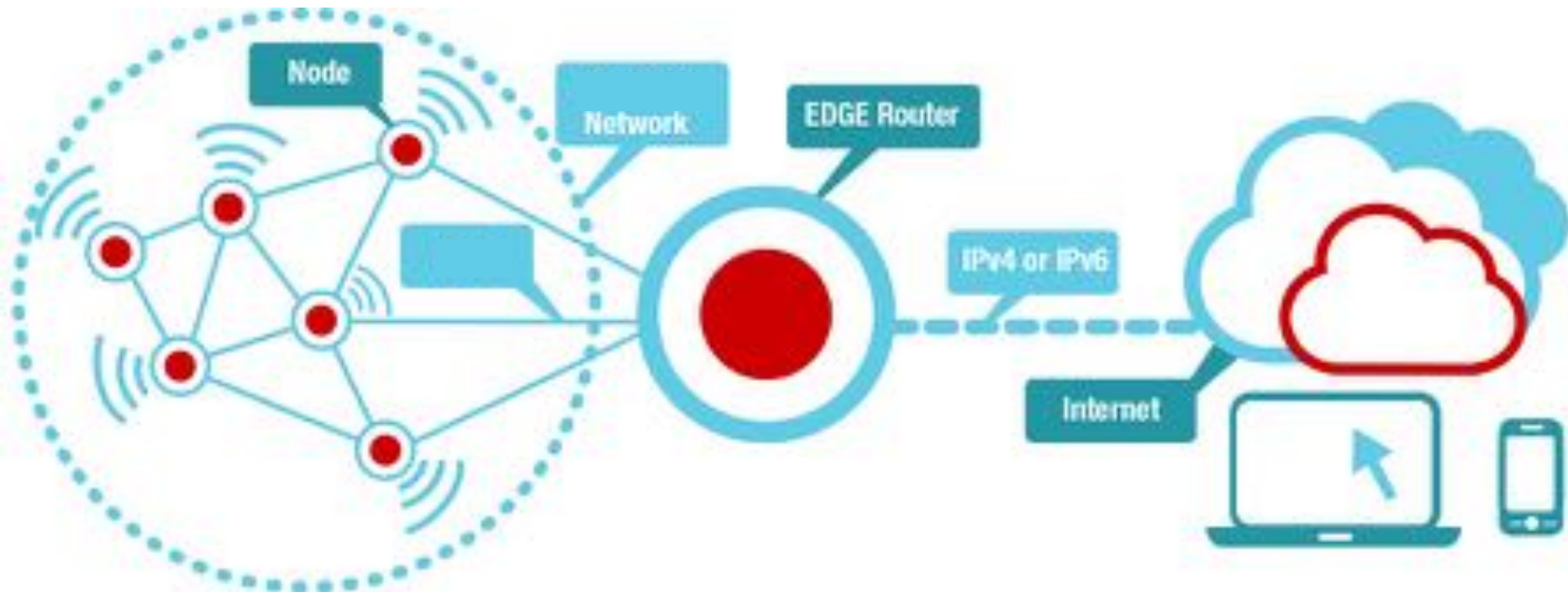
Frecuencias ISM (Bandas bajas)

Sub-1 GHz

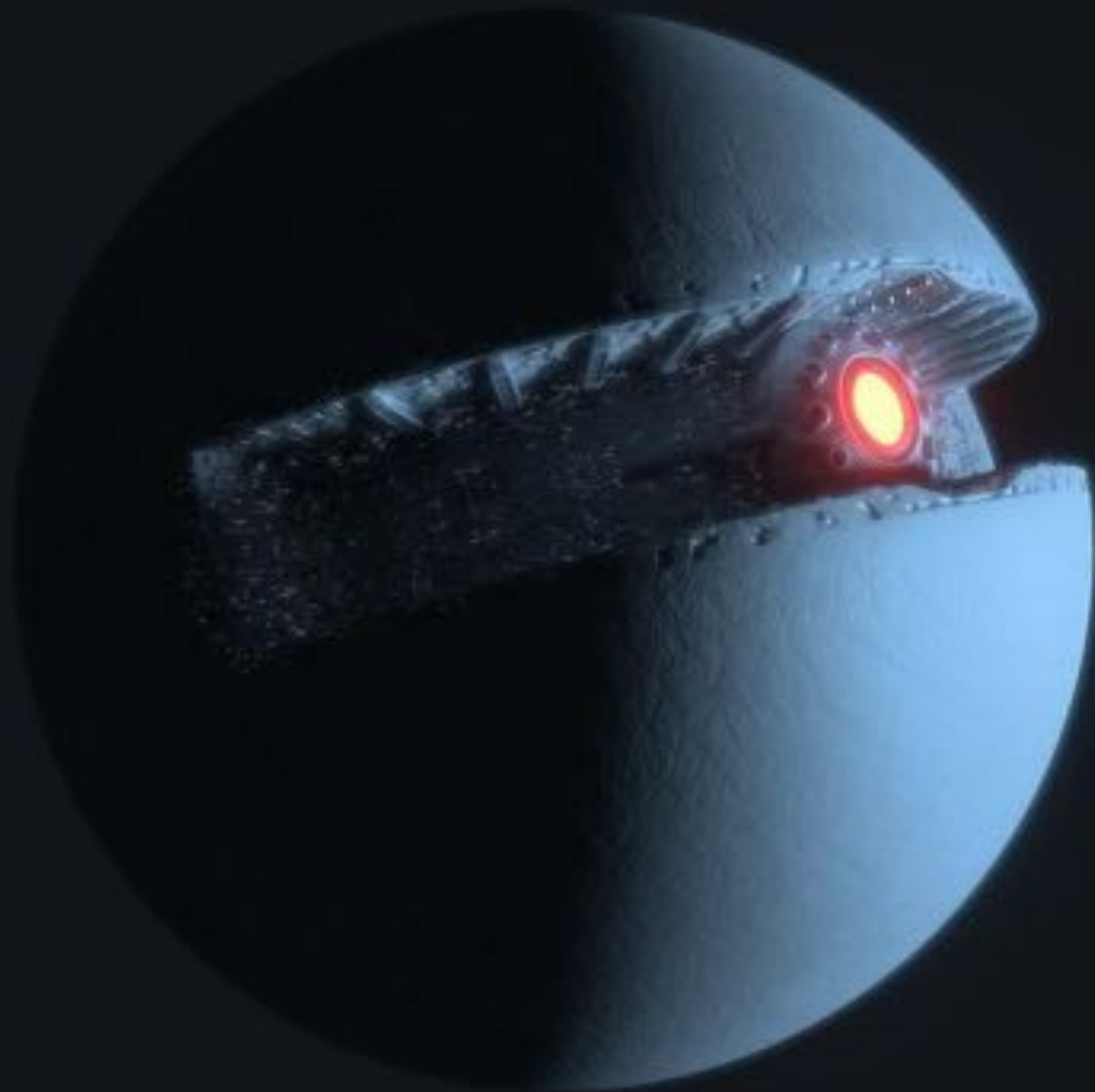
- 300 MHz (300-330) – US
- 433 MHz (433,05-433,790) – EU
- 868 MHz (863-870) – EU
- 915 MHz (902-928) – US
- Y los sospechosos habituales en bandas altas...
– 2.4 GHz & 5 GHz

Tecnologías propietarias, Bluetooth, Bluetooth Low Energy, LTE-M, Wi-Fi, Zigbee, Z-Wave, LoRaWAN, SigFox, 6LoWPAN, Weightless-N (Nwave), DASH7 (D7A)...

Arquitecturas IoT



Personal, Hogar, Empresarial, Industrial & Movilidad



Detección de nuevas tecnologías inalámbricas



iStupid (RootedCON 2013)

/Rooted°CON 2013

Managing the PNL in iOS



- iStupid (v0.9)
 - indescreet SSID Tool (for the) Unknown PNL (on) iOS Devices
- Generates beacons frames for one or multiple SSIDS (dictionary and brute force - *future*)
 - Multiple configuration options
 - Canal, SSID, BSSID, interval, rates, security settings...
- Allows to select the security settings
 - Open, WEP, WPA(2)-Personal & WPA(2)-Enterprise
 - WPA or WPA2 & TKIP or AES-CCMP (not relevant for iOS)
 - Loop

[http://www.dinosec.com/es/lab.html#iStupid \(v1.5\)](http://www.dinosec.com/es/lab.html#iStupid(v1.5))

idIoTas

- interacting (&)
- detecting
- Internet
- of
- Things
- assets



La vida es un cuento contado por un idiota,
lleno de ruido y de furia, que no tiene ningún
sentido

(William Shakespeare)



Sólo un idiota puede ser totalmente feliz.

(Mario Vargas Llosa)

akifrases.com



Él puede parecer un idiota y actuar como un
idiota, pero no se deje usted engañar, es
realmente un idiota.

(Groucho Marx)

akifrases.c



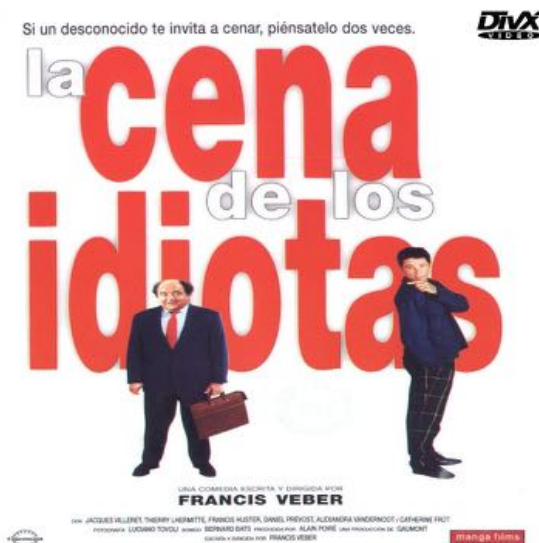
Existen dos maneras
de ser feliz en esta
vida, una es hacerse
el idiota y la otra
serlo.

Sigmund Freud

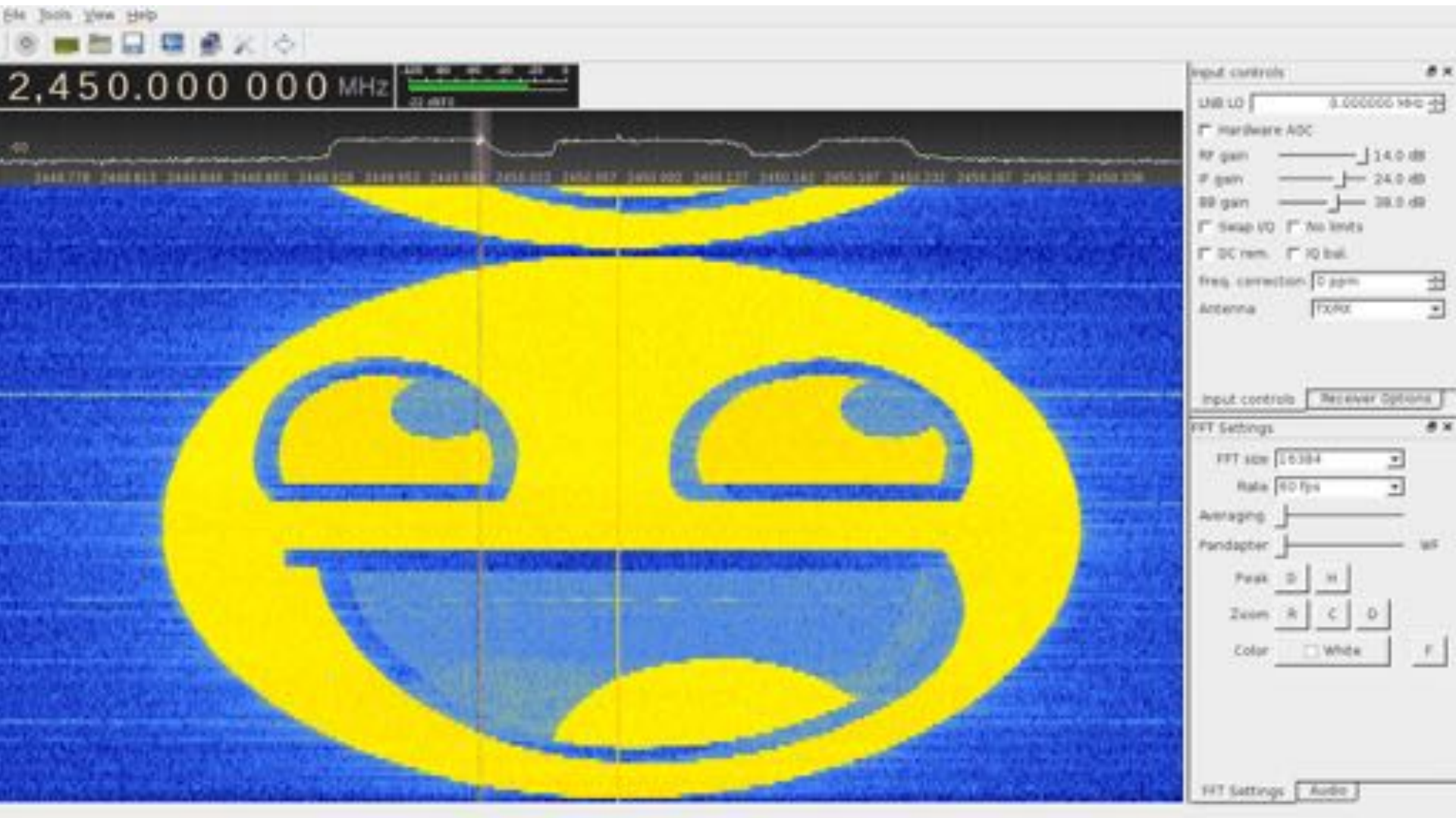
NFS

¿Cómo encontrar y convencer a los idloTas?

- Entorno modular para la interacción y detección de dispositivos IoT (idloTas) "desconocidos" con capacidades inalámbricas
 - idloTas
 - Tecnologías propietarias Sub-1 GHz, Bluetooth, Bluetooth Low Energy, Wi-Fi, Zigbee, Z-Wave...
 - ¿Qué hay en mi entorno?
- Caso concreto (Sub-1 GHz)



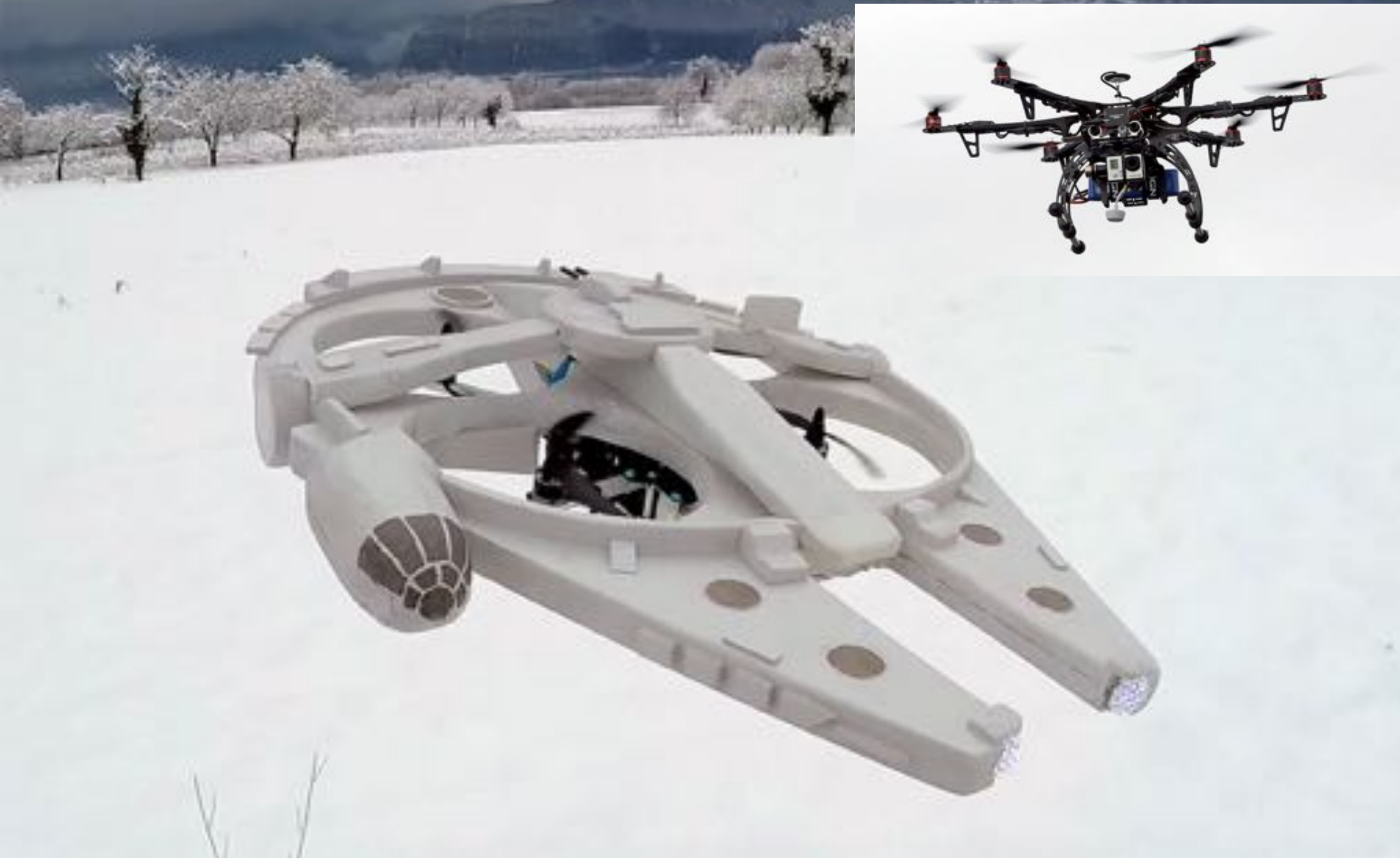
DEMO



DEMO



Conclusiones



El refranero español (RootedCON 2015)

/Rooted°CON 2015

El refranero español 

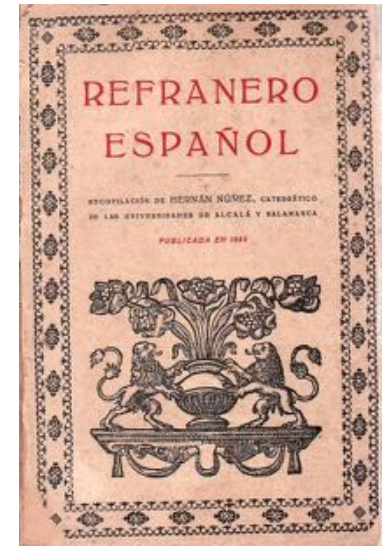


“Cuando las tecnologías
de tu vecino veas
peligrar...
...pon las tuyas a
actualizar”



El refranero español

“Bit que vuela...
...a la cazuela”



Credits

- Produced by: **Raúl Siles**
- Directed by: **Mónica Salas**
E & E
- Casting by: **Billones de idloTas**
- SDR Tools: **Michael Ossmann**
at1as
- Fan club: **Mamá, Tata, et. al.**
- Music by: **Siletes**
- Costume Designer: **DinoSec**

The End

¿Preguntas?

/Rooted[®]CON

§ DinoSec



A large logo in the center-left of the image featuring a stylized dollar sign with a dinosaur head inside it, followed by the text "DinoSec".

www.dinosec.com
[@dinosec](mailto:raul@dinosec.com)

Raúl Siles
raul@dinosec.com
[@raulsiles](https://twitter.com/raulsiles)