# MQTT, où comment l'infrastructure fragilise aussi les objets connectés

Renaud Lifchitz (renaud.lifchitz@digitalsecurity.fr)

Séminaire Cap'Tronic Paris – 17 novembre 2016

digital security | econocom

# Présentation de l'intervenant

- Renaud Lifchitz, consultant sécurité senior pour Digital Security

- Activités principales :
  - Tests d'intrusion et audits de sécurité
  - Recherche en sécurité informatique
  - Formations

- Centres d'intérêts :
  - Sécurité radio
  - Sécurité des protocoles (authentification, chiffrement, fuites d'information…)
  - Cryptographie
  - Développement sécurisé

# Activités de Digital Security

## CONSEIL

### Définition

En amont des projets :

- Stratégie, schéma directeur
- Cartographie des risques et plan de traitement
- Etudes prospectives et de cadrage
- Recherche d'opportunités

### Construction & mise en œuvre

Ingénierie sécurité :

- Politique & système de management (processus sécurité)
- Conduite du changement (formation, communication, sensibilisation)
- Intégration de la sécurité dans les projets
- Tests et recette des solutions

## AUDIT

### Evaluation

Au cœur des vérifications

- Tests d'intrusion
- Audits d'architecture
- Audits de conformité
- Audits de maturité
- Audit de code
- Audit de configuration
- Exercices en mode red team
- Préparation aux certifications
- Laboratoire de test et d'essai IoT

## CERT

### Maintien en condition de sécurité

Accompagnement opérationnel

- Réponse à incidents / Aide à la réaction (traitement des alertes, analyse forensic & post-incident)
- Contrôle continu
- Aide à la détection (veille, surveillance)

ISO 27001 Lead Auditor, ISO 27005 Risk Manager, ISO 22301 Lead Implementor, ITIL, CMMI

PASSI en cours

TF-CSIRT Trusted Introducer

# Le CERT-UBIK, premier CERT européen dédié à la sécurité des objets connectés

Le CERT-UBIK est doté d'un laboratoire dédié permettant d'adresser les nouvelles technologies de radiofréquence et les systèmes d'exploitation spécifiques aux objets connectés.


- Technologies de radiofréquence (Sigfox, LoRa, WiFi®, Bluetooth® et dérivés, ZigBee, Z-Wave, 6LoWPAN, ...)
- Systèmes d'exploitation spécifiques aux objets connectés (FreeRTOS, Tizen, TinyOS, …)
- Certifications Supelec et MatLab
- Bulletins de veille, évaluation, réponse à incidents, reverse engineering, ...


**OSIDO Mars 2016 sur la santé connectée**

## Qu'est-ce que l'OSIDO?

L'Observatoire de la sécurité de l'Internet des objets (OSIDO) est un livrable de veille **confidentielle** spécialisé sur la **sécurité** des objets connectés

## Une approche holistique de la sécurité

- Une sélection de l'actualité la plus pertinente présentée sous la forme de brèves : piratage d'objets connectés, solutions techniques envisagée, cadre réglementaire, etc.
- Un partenariat stratégique avec le cabinet d'avocat Garance Mathias spécialisé dans les nouvelles technologies pour l'actualité juridique
- Des « fiches pays » sur le développement de l'Internet des objets et leur impact sur la sécurité nationale
- Des comptes rendus de conférences apportant un éclairage précis sur les enjeux sécuritaires de l'IoT

- Un baromètre des risques analysant les menaces potentielles par secteur

- Un article de fond sur une thématique précise, enrichie par l'analyse de nos consultants permettant d'avoir une vue d'ensemble de la problématique énoncée.

- Des **fiches de vulnérabilités normées** sont proposées en option. Elles permettent d'identifier quelles sont les failles par secteur et leur niveau de criticité.

## Notre valeur ajoutée

- Une veille complète sur la sécurité des objets connectés **unique** sur le marché

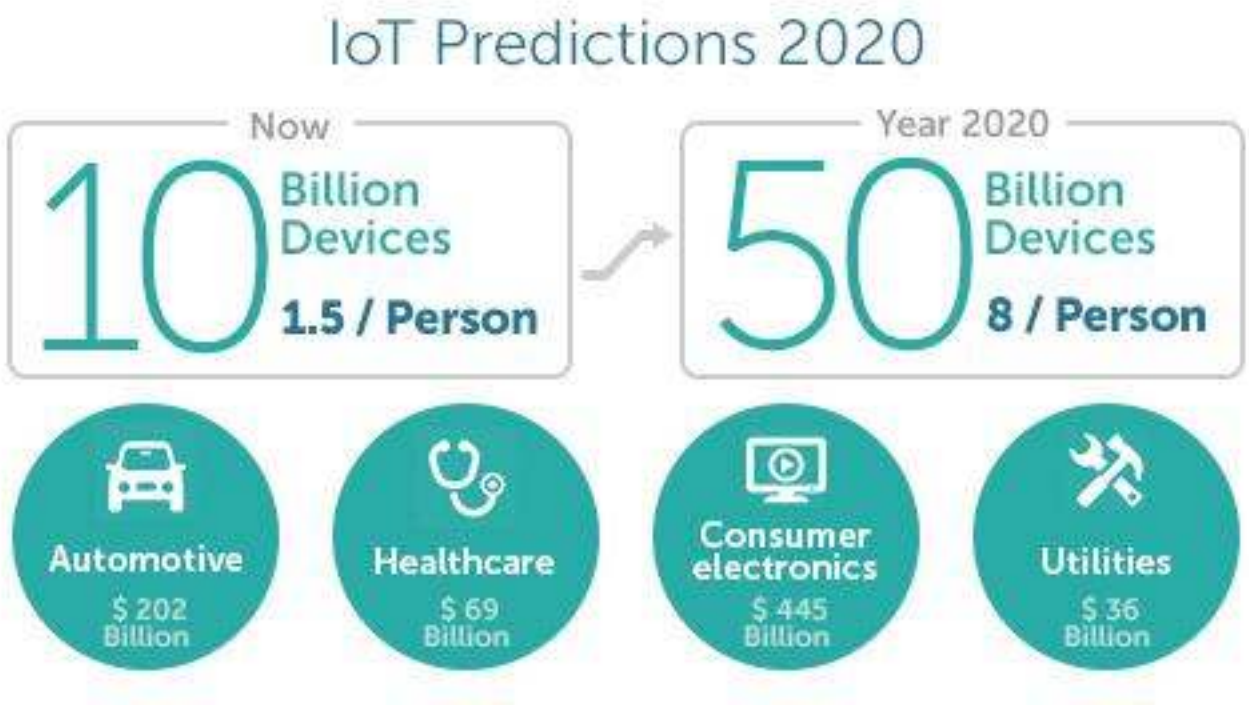
- La mise en place d'un **service hot-line** pour répondre aux questions de sécurité sur les objets connectés

- La possibilité de réaliser **un magazine Osido sur mesure** dédié à une problématique précise choisie par le client afin de permettre d'identifier les enjeux clés des secteurs analysés

# IoT : Un phénomène majeur

digital security

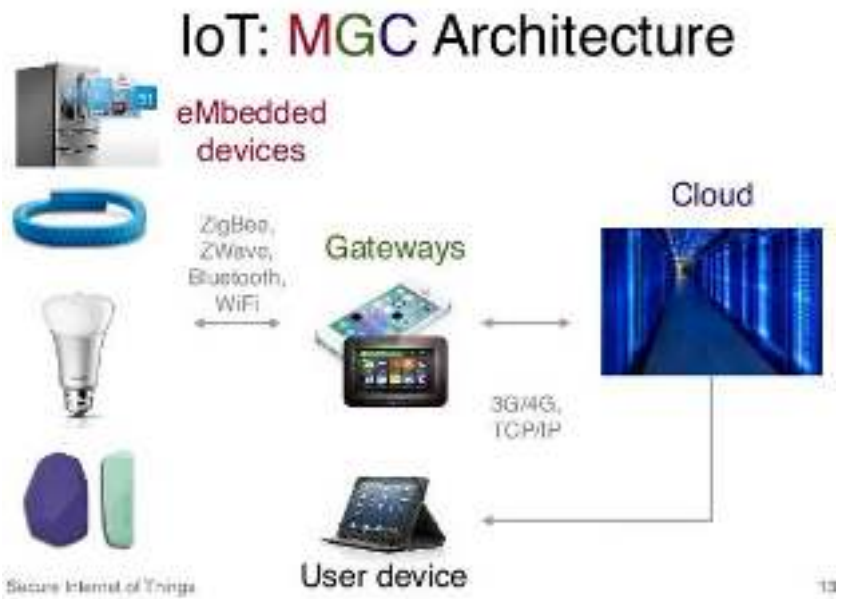
# Adoption des objets connectés




Source : iot-analytics.com

- Gartner :
  - « **D'ici la fin de l'année 2017, 20% des entreprises auront des équipes de sécurité dédiées** à la protection de leurs activités utilisant les services et équipements IoT »

# Une architecture complexe




Source : Mark Horowitz - Stanford Engineering - Securing the Internet of Things

- Des données à protéger dans une architecture distribuée et utilisant des dizaines de langages de programmation différents

*Un ensemble complexe à sécuriser*

# Points de vue des autorités

**Cybersécurité des objets connectés**

**Risques, bonnes pratiques et opportunités**

***Vincent Strubel***

**Agence Nationale de la Sécurité des Systèmes d'Information**

**17 juin 2015**

Source : Journée sur l'Internet des Objets et la Cybersécurité, CNAM

*Les principaux risques de sécurité IoT :*

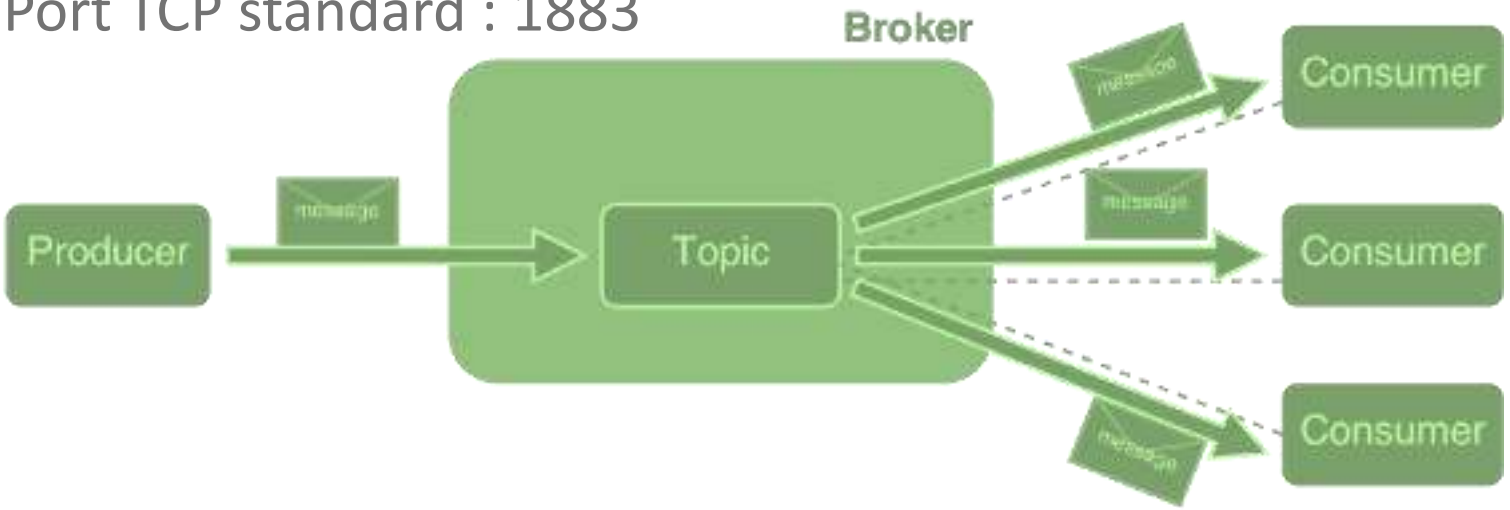
*Attaques destructives ou revendicatives, Espionnage, Sabotage, Détournement pour mener d'autres attaques*

# Qu’est-ce que le protocole MQTT ?

digital security

# Généralités

- MQTT : « Message Queuing Telemetry Transport », standard OASIS en plusieurs version
- Protocole d'envoi et réception de messages en flux continu (streaming)
- 2 types de clients :
  un « producer » et un « consumer »
- Un type de serveur : le « broker », intermédiaire entre tous les clients
- Port TCP standard : 1883

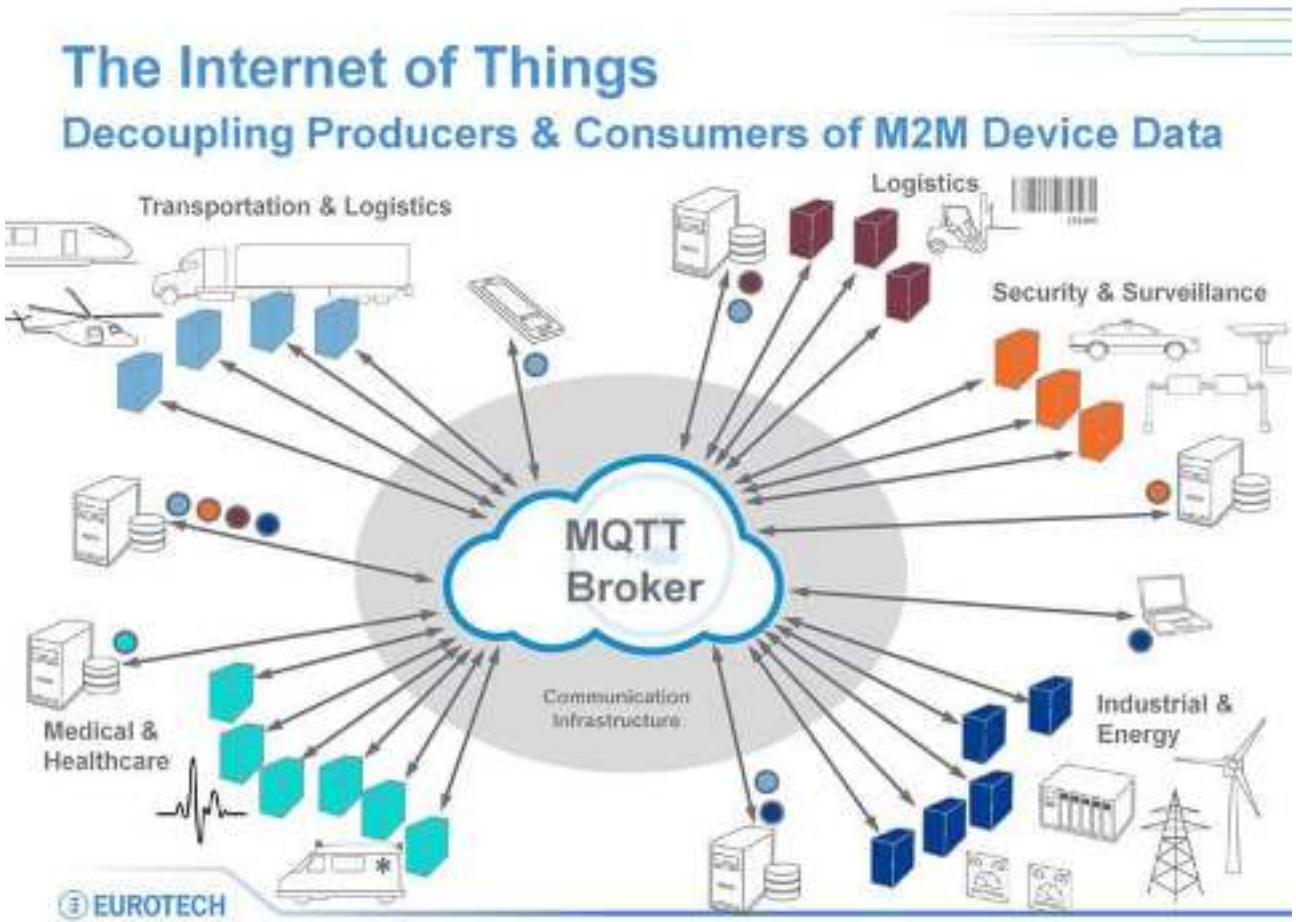


# Fonctionnalités

- Chaque « publisher » pousse au « broker » un « topic » (sujet) et des données associées (« data »)
- Chaque «  subscriber » s'abonne à certains « topics » et reçoit en push toute donnée concernant ses abonnements
- Les « topics » sont arborescents :
  /sujet1/sous-sujet1/…
  /sujet1/sous-sujet2/…
- Fonctionnalité de « wildcards » (jokers MQTT) :
  - + : joker un niveau
  - # : joker multi-niveau
- Topic particulier : $SYS (informations systèmes)

# Usages principaux

- Usage personnel : domotique



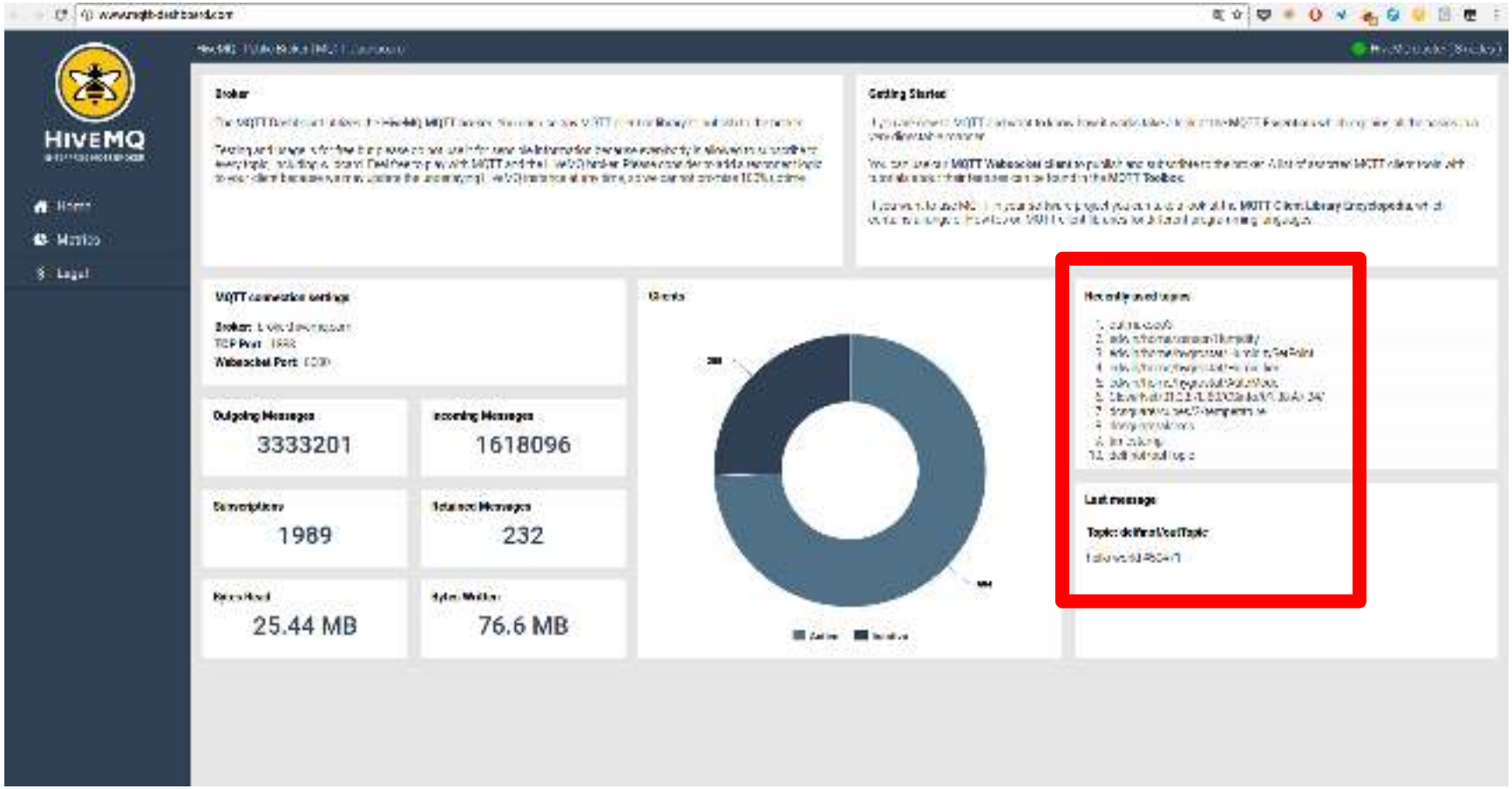
# Serveurs MQTT publics

- Serveurs de test/sandbox pour :
  - réaliser du prototypage (maquettes/PoC)
    sans configurer ni héberger de broker
  - réaliser des tests de compatibilité entre clients et brokers

- Exemples :
  - iot.eclipse.org
  - test.mosquitto.org
  - dev.rabbitmq.com
  - broker.hivemq.com
  - …

*Des données sensibles sont accessibles*
*sur beaucoup de serveurs MQTT publics*

# Serveurs MQTT publics



# Principaux brokers MQTT

- Eclipse Mosquitto (https://mosquitto.org)
- RabbitMQ (https://www.rabbitmq.com/), multi-protocole (AMQP, STOMP)

- HiveMQ, commercial

# Faiblesses récurrentes & exemples

digital security

# Informations souvent accessibles

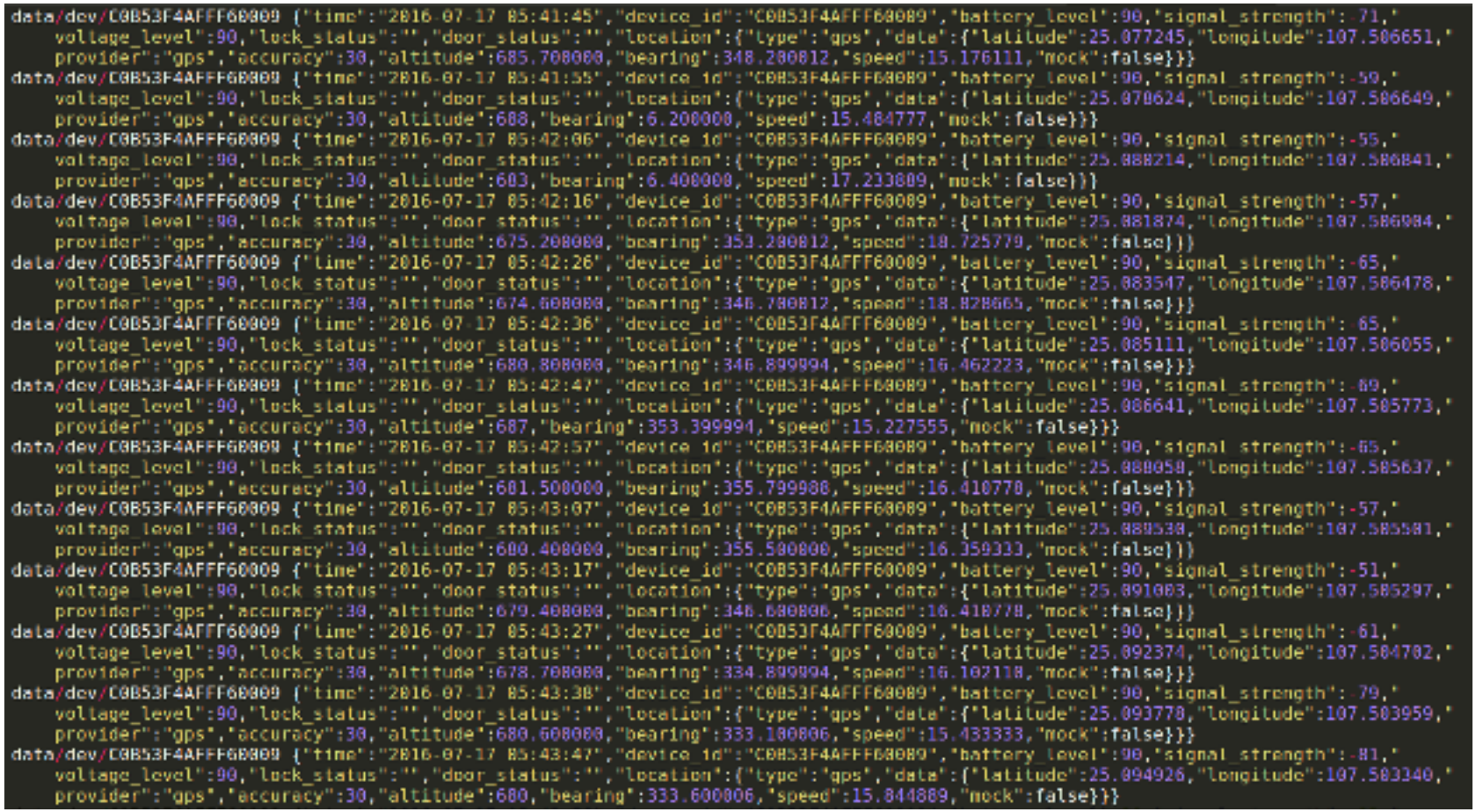
- Relevés de capteurs divers
  (température, hygrométrie, vent, domotique)
- Flux de messages LPWAN (Sigfox/LoRaWAN)

- Informations réglementées :
  - Informations à caractère personnel (identifiants : logins, IP, adresses MAC, noms et prénoms, numéros de téléphone, adresses e-mail, géolocalisations…)
  - Informations médicales
    (rythme cardiaque, tension, taux de glucose, ...)
  - Informations financières (flux de transactions)
  - Informations à diffusion restreinte (DR)

# Informations insolites accessibles

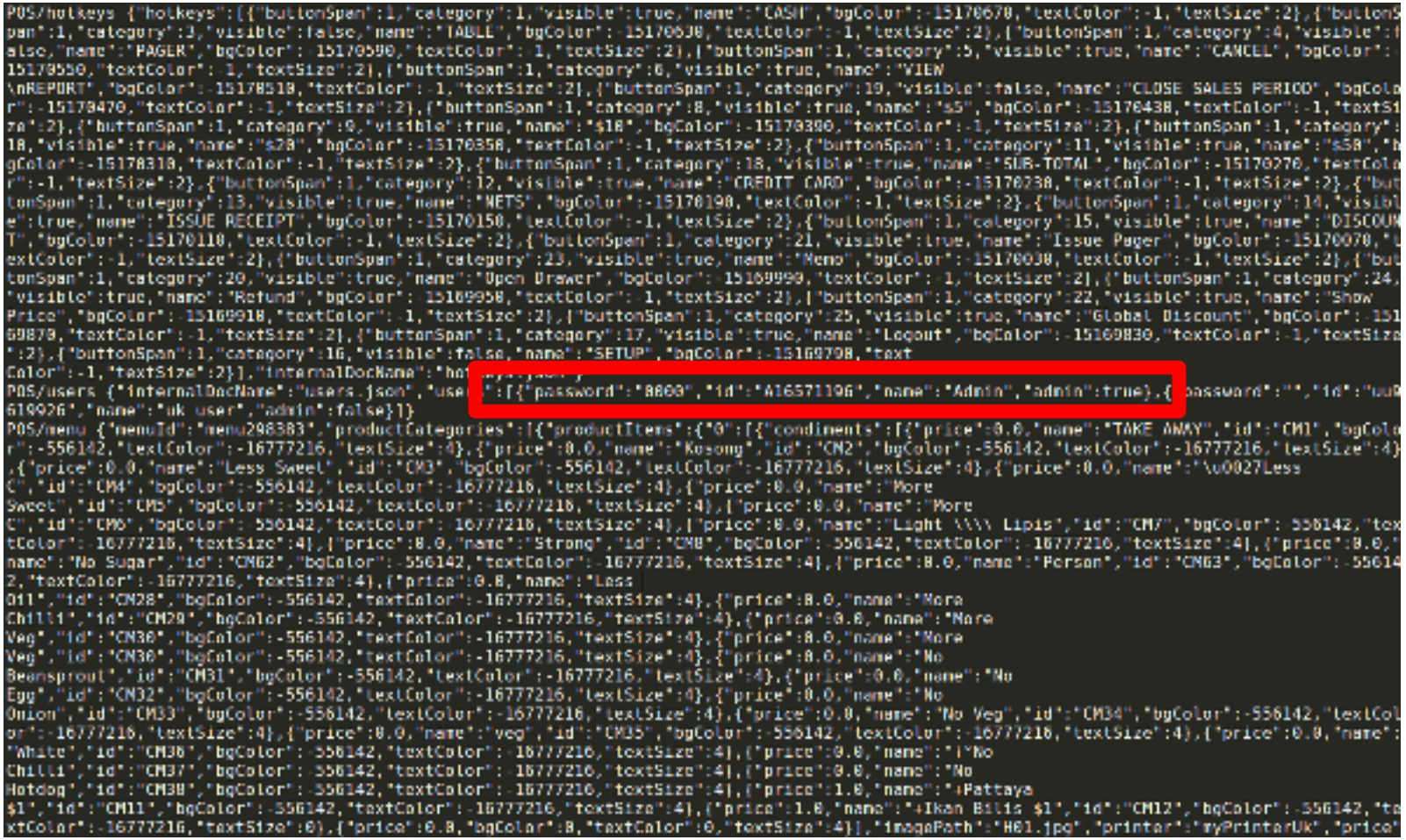
- Propriété intellectuelle :
  données de prototypes d'objets IoT (laboratoires de GAFA)
- Questions et réponses à des jeux concours
- Réveil connecté à affichage personnalisable
  (lecture et écriture de messages possible !)

# Exemples de services MQTT exposés



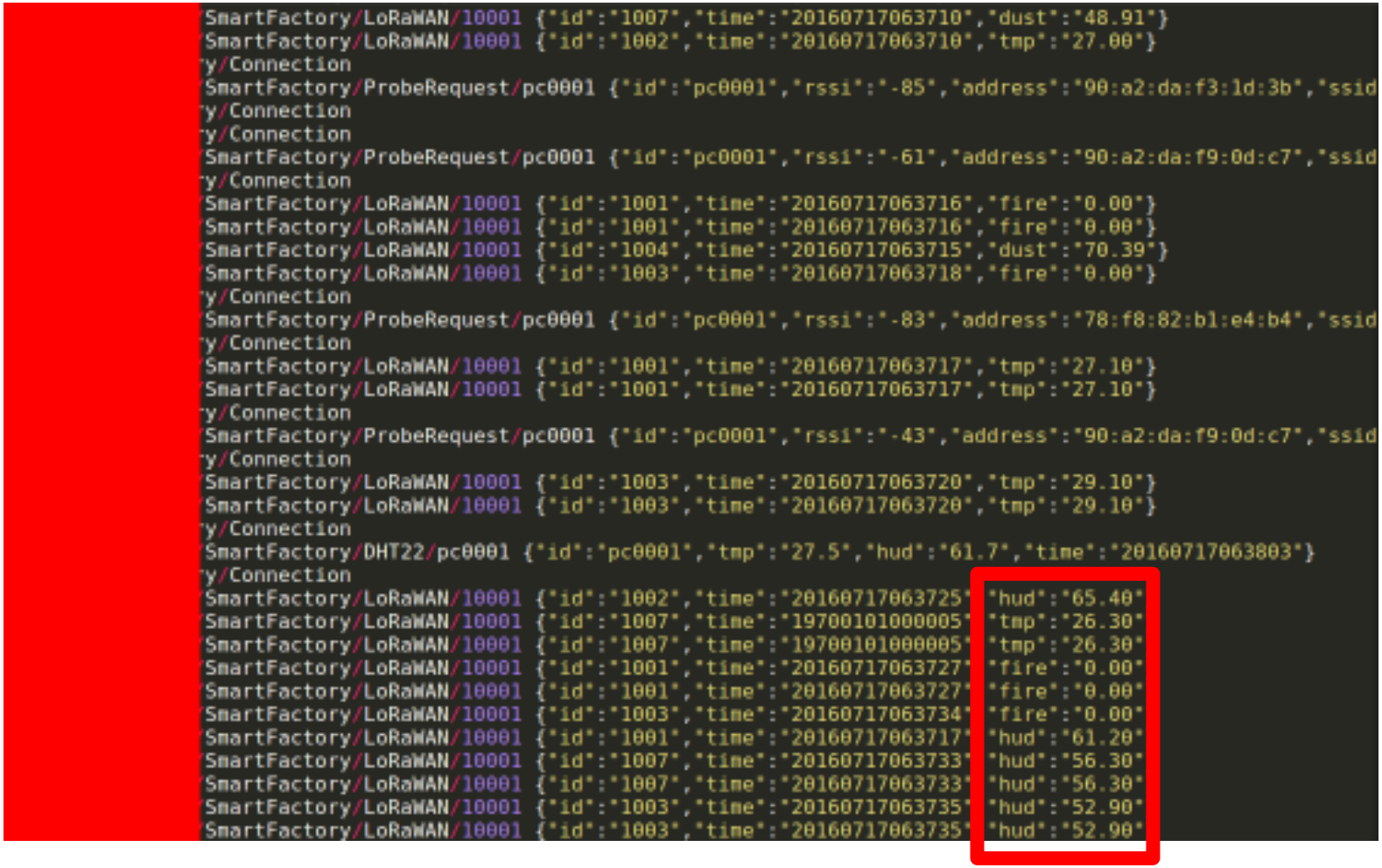

Ballon sonde en Chine ?

# Exemples de services MQTT exposés




Caisse enregistreuse britannique ?

# Exemples de services MQTT exposés

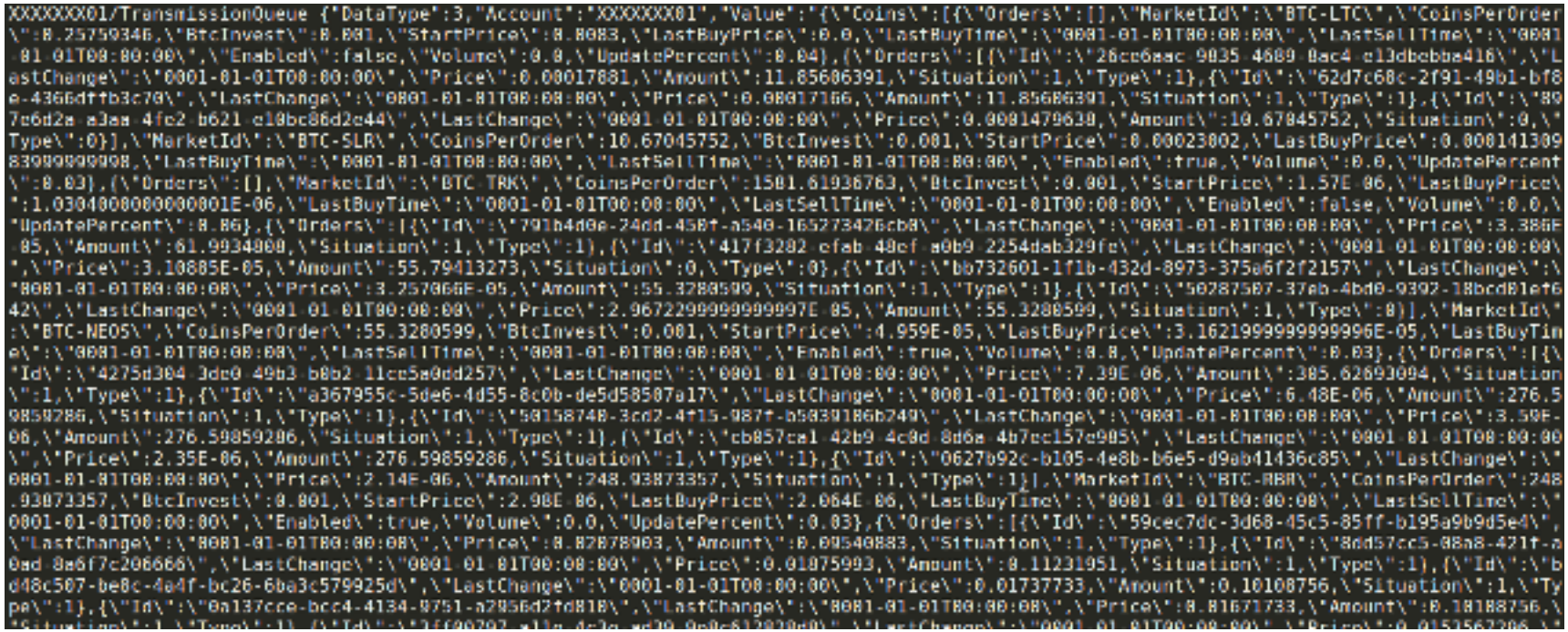



Usine connectée LoRaWAN en Corée ?

# Exemples de services MQTT exposés


Compteur d'énergie (smartmeter) et sonde météo BLE ?

# Exemples de services MQTT exposés




File de traitement de transactions financières Bitcoin

# Défaut de chiffrement

- Peu d'utilisation de SSL/TLS :
  - Difficulté de configuration côté broker
  - Utilisation lourde de certificats côté client

- Les informations MQTT et les authentifications se retrouvent exposés

- Un attaquant sur le même réseau que le client ou le broker peut facilement écouter le flux
- Un attaquant entre le client et le broker est aussi susceptible de l'écouter

*Les flux et authentifications MQTT transitent souvent en clair sur les réseaux*

# Défaut d'authentification

- Beaucoup de brokers sans authentification
- Beaucoup d'applications avec mot de passe unique écrit en dur dans le code, côté client
- Les utilisateurs ont souvent tous les mêmes droits et ne sont pas identifiables

*Utilisateurs mal authentifiés sur de nombreux brokers MQTT*

# Défaut de cloisonnement

- Cloisonnement entre utilisateurs délicat avec MQTT
- Le filtrage par topic selon les identifiants n'est pas possible chez de nombreux brokers
- Conséquence : à l'aide de jokers MQTT (« wildcards »), n'importe quel utilisateur peut lire voire écrire à la place d'un autre utilisateur

*Peu de brokers permettent d'isoler correctement les clients*

# Usurpation & falsification de données

- Dans de nombreux cas (défaut d'authentification ou de cloisonnement suffisant), un « suscriber » peut se faire passer pour un « publisher » : usurpation

- La falsification de données est relativement aisée : fausses alertes, dénis de service et corruption de données métiers

# Durcissement d’un service MQTT

digital security

# Principe de sécurité en profondeur

- Durcissement à 3 niveaux :
  - niveau réseau : sécurité physique et/ou VPN
  - niveau transport : SSL/TLS
  - niveau applicatif :
    - ↪ authentification applicative : simple (standard) ou à double facteur
    - ↪ chiffrement de données applicatif
    - ↪ cloisonnement applicatifs (implémentation et tests non aisés)

# Contact

digital security

Renaud LIFCHITZ
Consultant Sécurité Senior
renaud.lifchitz@digitalsecurity.fr
+ 33 (0)1 70 83 85 72

Thomas GAYET
Directeur du CERT-UBIK
thomas.gayet@digitalsecurity.fr
+ 33 (0)1 70 83 85 51

## Sécurité de l'Internet des Objets