



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

Renaud Lifchitz (renaud.lifchitz@digitalsecurity.fr)

Séminaire Cap'Tronic Paris – 17 novembre 2016

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)



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, ...

Observatoire de la Sécurité de l'Internet des Objets

digital security

www.digitalsecurity.fr | MARS 2016

VEILLE STRATÉGIQUE

Le développement IoT analyse par
des spécialistes de la sécurité

DEVELOPPEMENT REGIONAL

De l'Internet des objets

VEILLE SÉCURITAIRE

Technique et opérationnelle

BAROMÈTRE DES RISQUES

Panorama des attaques et
des menaces par secteur

La santé connectée : opportunités et dangers

FOCUS PAYS

Le développement de l'IoT en Chine

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

OSIDO Mars 2016 sur la santé connectée

- ◆ 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

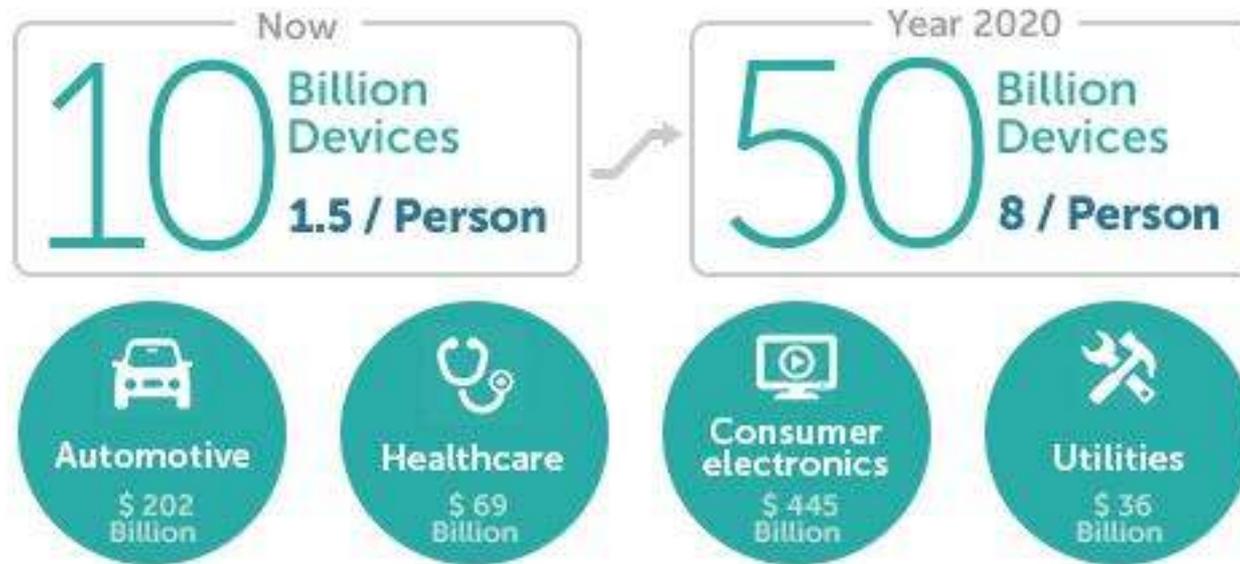
- ◆ Une veille complète sur la sécurité des objets connectés **unique** sur le marché
- ◆ La mise en place d'un **service hot-line** pour répondre aux questions de sécurité sur les objets connectés
- ◆ La possibilité de réaliser **un magazine Osido sur mesure** dédié à une problématique précise choisie par le client afin de permettre d'identifier les enjeux clés des secteurs analysés

IoT : Un phénomène majeur

digital security

Adoption des objets connectés

IoT Predictions 2020

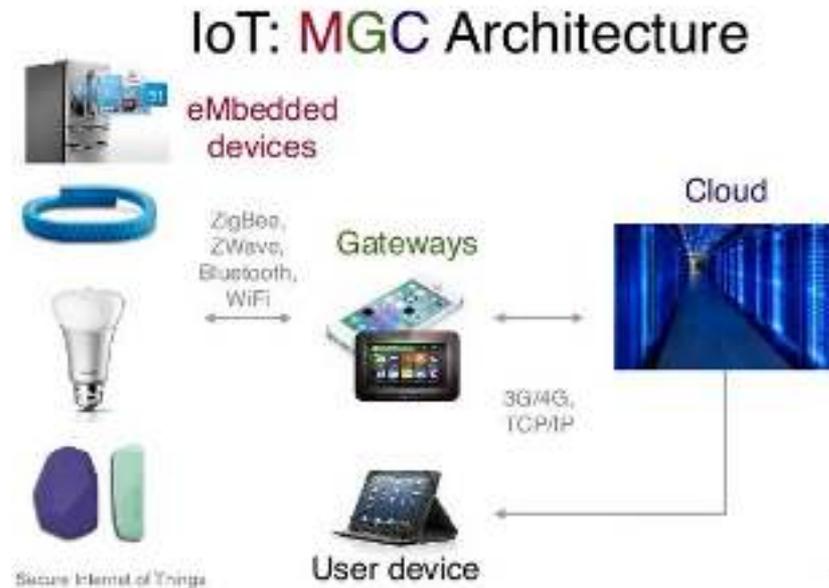


Source : iot-analytics.com

■ 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 :

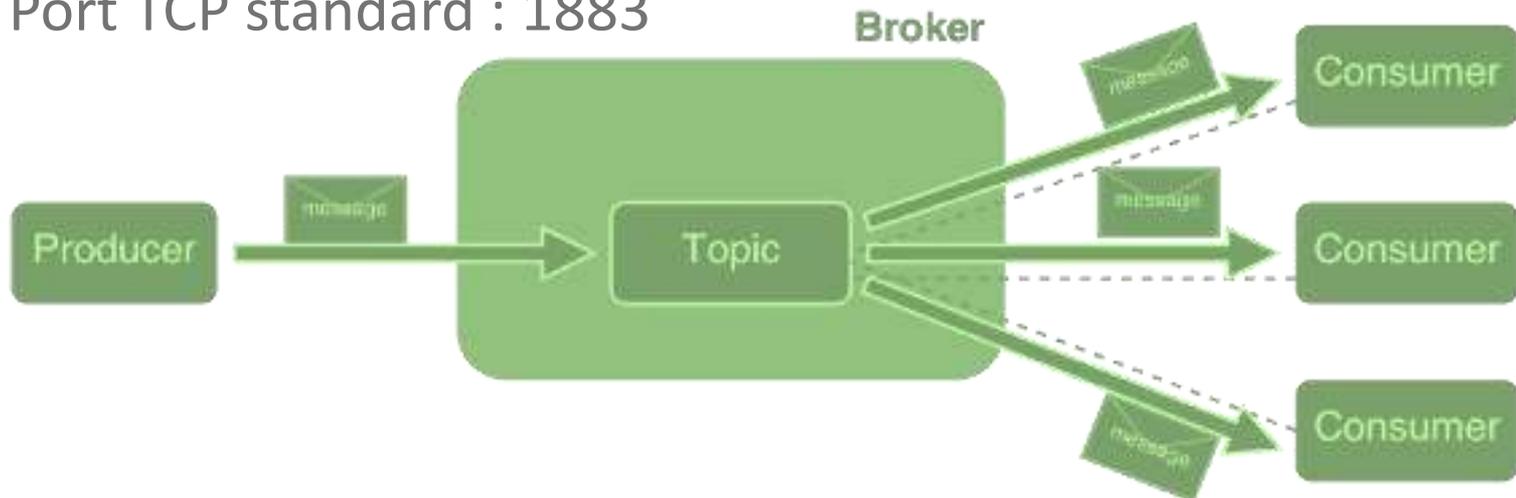
*Attaques destructives ou revendicatives, Espionnage, Sabotage,
Détournement pour mener d'autres attaques*

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



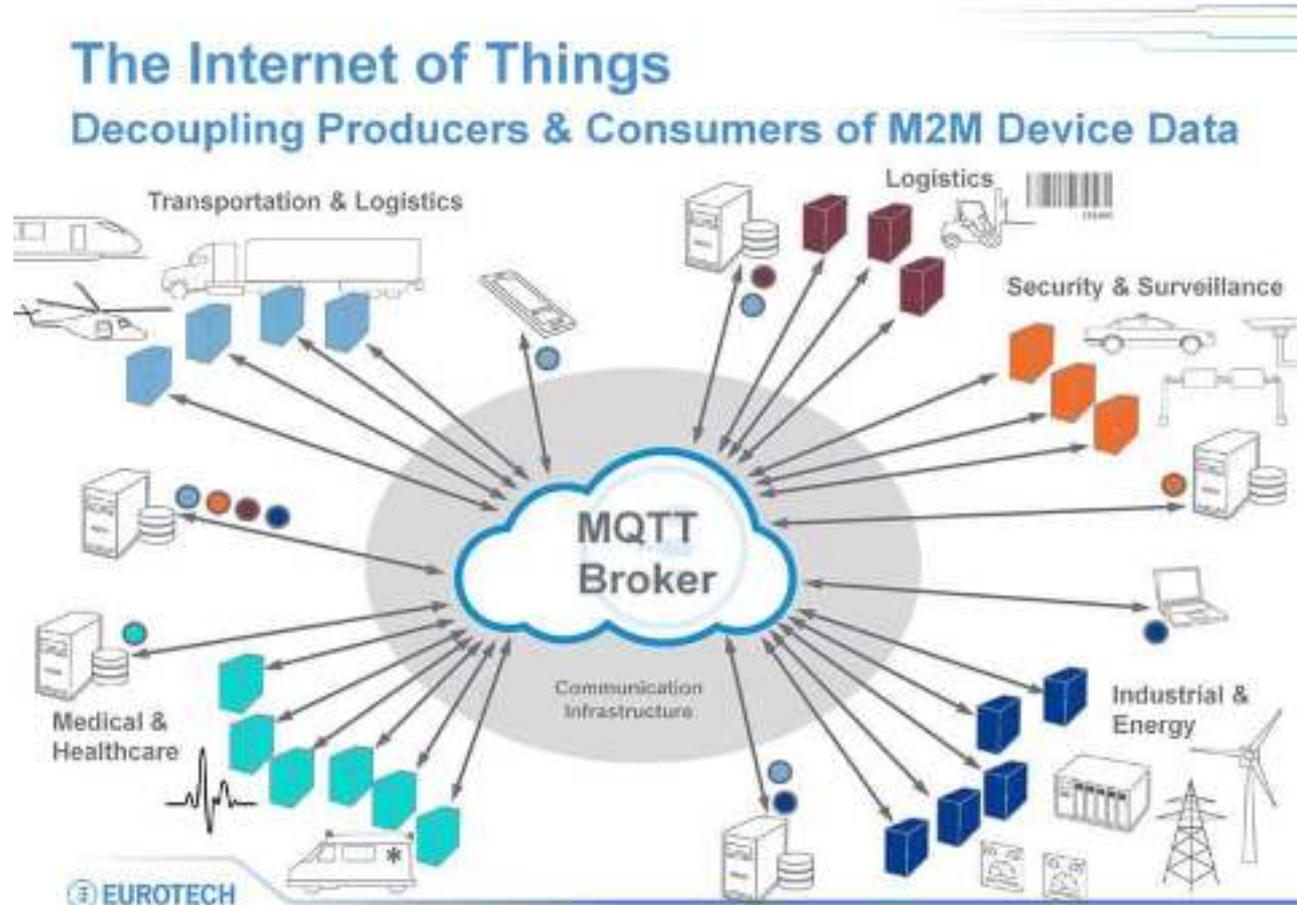
Fonctionnalités

- 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

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

```
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:41:45","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":71,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.077245,"longitude":107.506651,"provider":"gps","accuracy":30,"altitude":685.708000,"bearing":348.200012,"speed":15.176111,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:41:55","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":59,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.070624,"longitude":107.506649,"provider":"gps","accuracy":30,"altitude":688,"bearing":6.200000,"speed":15.484777,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:42:06","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":55,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.088214,"longitude":107.506841,"provider":"gps","accuracy":30,"altitude":603,"bearing":6.400000,"speed":17.230009,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:42:16","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":57,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.081874,"longitude":107.506084,"provider":"gps","accuracy":30,"altitude":675.208000,"bearing":353.200012,"speed":18.725779,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:42:26","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":65,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.083547,"longitude":107.506478,"provider":"gps","accuracy":30,"altitude":674.000000,"bearing":346.700012,"speed":18.028665,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:42:36","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":65,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.085111,"longitude":107.506055,"provider":"gps","accuracy":30,"altitude":680.000000,"bearing":346.000000,"speed":16.462223,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:42:47","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":69,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.086641,"longitude":107.505773,"provider":"gps","accuracy":30,"altitude":687,"bearing":353.399994,"speed":15.227555,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:42:57","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":65,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.088050,"longitude":107.505637,"provider":"gps","accuracy":30,"altitude":601.500000,"bearing":355.799980,"speed":16.410770,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:43:07","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":57,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.089530,"longitude":107.505501,"provider":"gps","accuracy":30,"altitude":600.400000,"bearing":355.500000,"speed":16.359333,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:43:17","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":51,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.091003,"longitude":107.505297,"provider":"gps","accuracy":30,"altitude":679.000000,"bearing":348.000000,"speed":16.418770,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:43:27","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":61,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.092374,"longitude":107.504702,"provider":"gps","accuracy":30,"altitude":678.700000,"bearing":334.000000,"speed":16.102118,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:43:38","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":79,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.093770,"longitude":107.503959,"provider":"gps","accuracy":30,"altitude":680.000000,"bearing":333.100000,"speed":15.433333,"mock":false}}}
data/dev/C0B53F4AFFF60009 {"time":"2016-07-17 05:43:47","device_id":"C0B53F4AFFF60009","battery_level":90,"signal_strength":81,"voltage_level":90,"lock_status":"","door_status":"","location":{"type":"gps","data":{"latitude":25.094926,"longitude":107.503340,"provider":"gps","accuracy":30,"altitude":680,"bearing":333.600006,"speed":15.844889,"mock":false}}}
```

Ballon sonde en Chine ?

Exemples de services MQTT exposés

```
SmartFactory/LoRaWAN/10001 {"id":"1007","time":"20160717063710","dust":"48.91"}
SmartFactory/LoRaWAN/10001 {"id":"1002","time":"20160717063710","tmp":"27.00"}
y/Connection
SmartFactory/ProbeRequest/pc0001 {"id":"pc0001","rssi":"-85","address":"90:a2:da:f3:1d:3b","ssid
y/Connection
y/Connection
SmartFactory/ProbeRequest/pc0001 {"id":"pc0001","rssi":"-61","address":"90:a2:da:f9:0d:c7","ssid
y/Connection
SmartFactory/LoRaWAN/10001 {"id":"1001","time":"20160717063716","fire":"0.00"}
SmartFactory/LoRaWAN/10001 {"id":"1001","time":"20160717063716","fire":"0.00"}
SmartFactory/LoRaWAN/10001 {"id":"1004","time":"20160717063715","dust":"70.39"}
SmartFactory/LoRaWAN/10001 {"id":"1003","time":"20160717063718","fire":"0.00"}
y/Connection
SmartFactory/ProbeRequest/pc0001 {"id":"pc0001","rssi":"-83","address":"78:f8:82:b1:e4:b4","ssid
y/Connection
SmartFactory/LoRaWAN/10001 {"id":"1001","time":"20160717063717","tmp":"27.10"}
SmartFactory/LoRaWAN/10001 {"id":"1001","time":"20160717063717","tmp":"27.10"}
y/Connection
SmartFactory/ProbeRequest/pc0001 {"id":"pc0001","rssi":"-43","address":"90:a2:da:f9:0d:c7","ssid
y/Connection
SmartFactory/LoRaWAN/10001 {"id":"1003","time":"20160717063720","tmp":"29.10"}
SmartFactory/LoRaWAN/10001 {"id":"1003","time":"20160717063720","tmp":"29.10"}
y/Connection
SmartFactory/DHT22/pc0001 {"id":"pc0001","tmp":"27.5","hud":"61.7","time":"20160717063803"}
y/Connection
SmartFactory/LoRaWAN/10001 {"id":"1002","time":"20160717063725","hud":"65.40"}
SmartFactory/LoRaWAN/10001 {"id":"1007","time":"19700101000005","tmp":"26.30"}
SmartFactory/LoRaWAN/10001 {"id":"1007","time":"19700101000005","tmp":"26.30"}
SmartFactory/LoRaWAN/10001 {"id":"1001","time":"20160717063727","fire":"0.00"}
SmartFactory/LoRaWAN/10001 {"id":"1001","time":"20160717063727","fire":"0.00"}
SmartFactory/LoRaWAN/10001 {"id":"1003","time":"20160717063734","fire":"0.00"}
SmartFactory/LoRaWAN/10001 {"id":"1001","time":"20160717063717","hud":"61.20"}
SmartFactory/LoRaWAN/10001 {"id":"1007","time":"20160717063733","hud":"56.30"}
SmartFactory/LoRaWAN/10001 {"id":"1007","time":"20160717063733","hud":"56.30"}
SmartFactory/LoRaWAN/10001 {"id":"1003","time":"20160717063735","hud":"52.90"}
SmartFactory/LoRaWAN/10001 {"id":"1003","time":"20160717063735","hud":"52.90"}
```

Usine connectée LoRaWAN en Corée ?

Exemples de services MQTT exposés

```
gateway-topics ["device/PowerBlade/c098e5700089", "device/BLEES/c098e5300054", "device/BLEES/c098e530005d", "device/BLEES/c098e5300009", "device/BLEES/c098e5300036", "device/Blink/c098e590001e", "device/PowerBlade/c098e5700090", "device/PowerBlade/c098e5700009"]
gateway-data {"device": "PowerBlade", "sequence_number": 432635, "rms_voltage": "118.58", "power": "0.00", "apparent_power": "92.44", "energy": "1187.83", "power_factor": "0.00", "id": "c098e5700089", "meta": {"received_time": "2016-07-16T21:43:16.141Z", "device_id": "c098e5700089", "receiver": "ble-gateway", "gateway_id": "d0:5f:b8:e4:40:5d"}}
device/PowerBlade/c098e5700009 {"device": "PowerBlade", "sequence_number": 432635, "rms_voltage": "118.58", "power": "0.00", "apparent_power": "92.44", "energy": "1187.83", "power_factor": "0.00", "id": "c098e5700089", "meta": {"received_time": "2016-07-16T21:43:16.141Z", "device_id": "c098e5700089", "receiver": "ble-gateway", "gateway_id": "d0:5f:b8:e4:40:5d"}}
ble-advertisements {"globalHashedAddress": "9e", "localHashedAddress": "d96025e7b4e0011ba7230b6641d141073d0ad179303d2e4f910ee8292f57c06a", "address": "c098e5700089", "rssi": -62, "receivedTime": "2016-07-16T21:43:16.163Z"}
ble-advertisements {"globalHashedAddress": "8c", "localHashedAddress": "8e1ed989cd4547f1a73164a567da988c9dae2becf7a84fd08752c4d1d8db15b68", "address": "c098e570008f", "rssi": 60, "receivedTime": "2016-07-16T21:43:16.249Z"}
gateway-data {"device": "PowerBlade", "sequence_number": 432621, "rms_voltage": "118.20", "power": "1.13", "apparent_power": "16.78", "energy": "1168.87", "power_factor": "0.07", "id": "c098e5700090", "meta": {"received_time": "2016-07-16T21:43:16.288Z", "device_id": "c098e5700090", "receiver": "ble-gateway", "gateway_id": "d0:5f:b8:e4:40:5d"}}
device/PowerBlade/c098e5700090 {"device": "PowerBlade", "sequence_number": 432621, "rms_voltage": "118.20", "power": "1.13", "apparent_power": "16.78", "energy": "1168.87", "power_factor": "0.07", "id": "c098e5700090", "meta": {"received_time": "2016-07-16T21:43:16.288Z", "device_id": "c098e5700090", "receiver": "ble-gateway", "gateway_id": "d0:5f:b8:e4:40:5d"}}
acceleration_advertisement": false, "acceleration_interval": false, "sequence_number": -1, "id": "c098e5300054", "meta": {"received_time": "2016-07-16T21:43:16.306Z", "device_id": "c098e5300054", "receiver": "ble-gateway", "gateway_id": "d0:5f:b8:e4:40:5d"}}
device/BLEES/c098e5300054 {"device": "BLEES", "pressure_pascals": 100502.4, "humidity_percent": 32.07, "temperature_celcius": 22.95, "light_lux": 31, "acceleration_advertisement": false, "acceleration_interval": false, "sequence_number": -1, "id": "c098e5300054", "meta": {"received_time": "2016-07-16T21:43:16.306Z", "device_id": "c098e5300054", "receiver": "ble-gateway", "gateway_id": "d0:5f:b8:e4:40:5d"}}
ble-advertisements {"globalHashedAddress": "99", "localHashedAddress": "759493bb3c5f394787805948d0a4cd6c3751cddc85c5543ce5dcb792a5a0751f", "address": "c098e5700090", "rssi": -62, "receivedTime": "2016-07-16T21:43:16.321Z"}
ble-advertisements {"globalHashedAddress": "66", "localHashedAddress": "a4a028390474d08554d45811887c1e486daf28875141ed26980096272f12ec12", "address": "c098e5300054", "rssi": 81, "receivedTime": "2016-07-16T21:43:16.325Z"}
ble-advertisements {"globalHashedAddress": "9e", "localHashedAddress": "d96025e7b4e0011ba7230b6641d141073d0ad179303d2e4f910ee8292f57c06a", "address": "c098e5700089", "rssi": -62, "receivedTime": "2016-07-16T21:43:16.366Z"}
ble-advertisements {"globalHashedAddress": "13", "localHashedAddress": "ab8a68f0c3a00a1f0c2a7b84bfc447bb56d81d1961e6eb9176e5524722e278a3", "address": "c098e5300036", "rssi": 81, "receivedTime": "2016-07-16T21:43:16.452Z"}
gateway-data {"device": "BLEES", "pressure_pascals": 100672.7, "humidity_percent": 34.52, "temperature_celcius": 22.39, "light_lux": 37, "acceleration_advertisement": false, "acceleration_interval": false, "sequence_number": -1, "id": "c098e5300036", "meta": {"received_time": "2016-07-16T21:43:16.448Z", "device_id": "c098e5300036", "receiver": "ble-gateway", "gateway_id": "d0:5f:b8:e4:40:5d"}}
```

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

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 « subscriber » 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

