La sécurité des objets connectés à la lumière de l'actualité

Patrick CHAMBET – RSSI

Arnaud GORIUS – RSSI GSF

CLUSIR PACA - CESIN

Sommaire

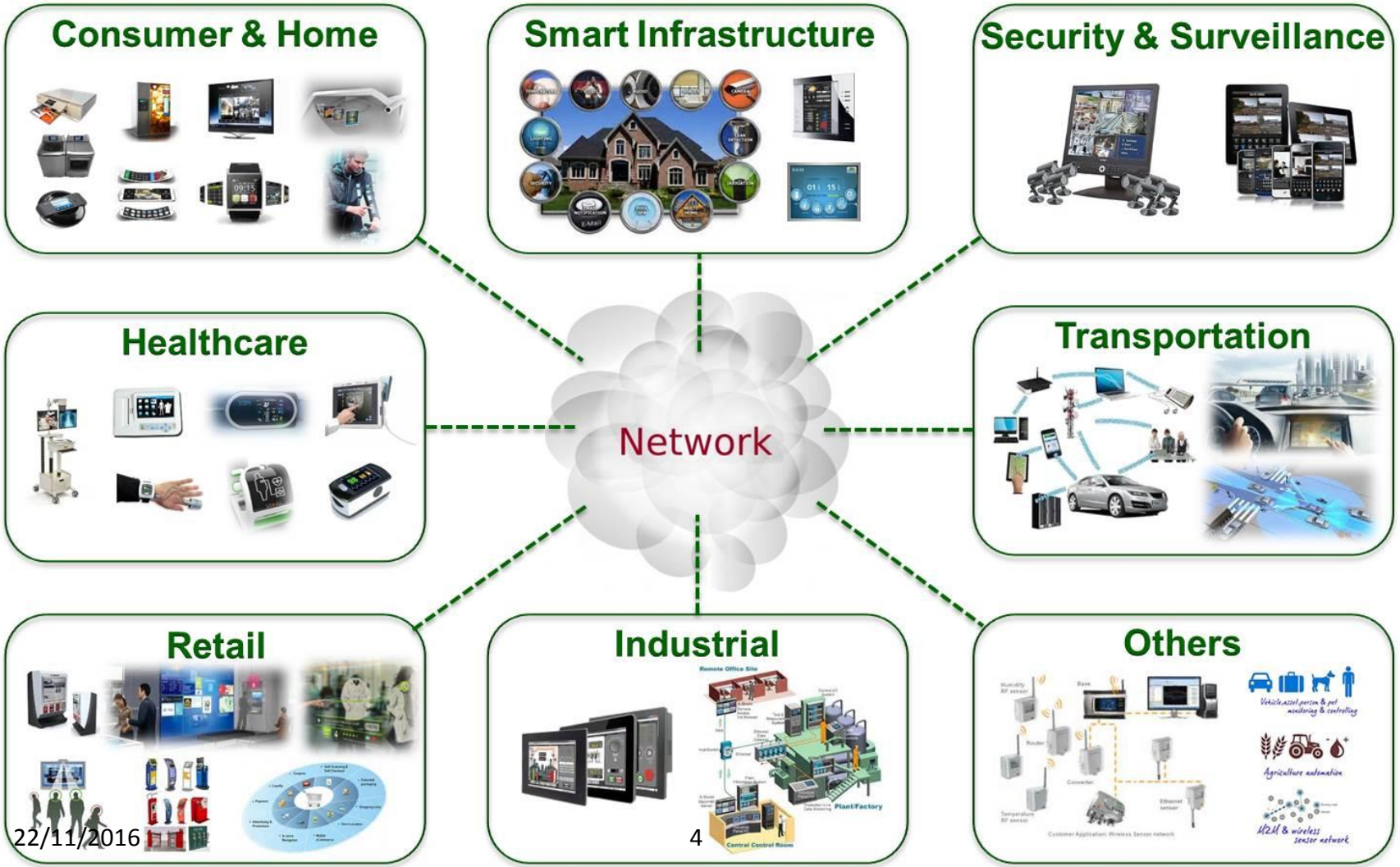
1. Les objets connectés et l'IoT
2. La sécurité des objets connectés
3. Quelques attaques récentes
4. Mesures de sécurisation

Les objets connectés et l'IoT

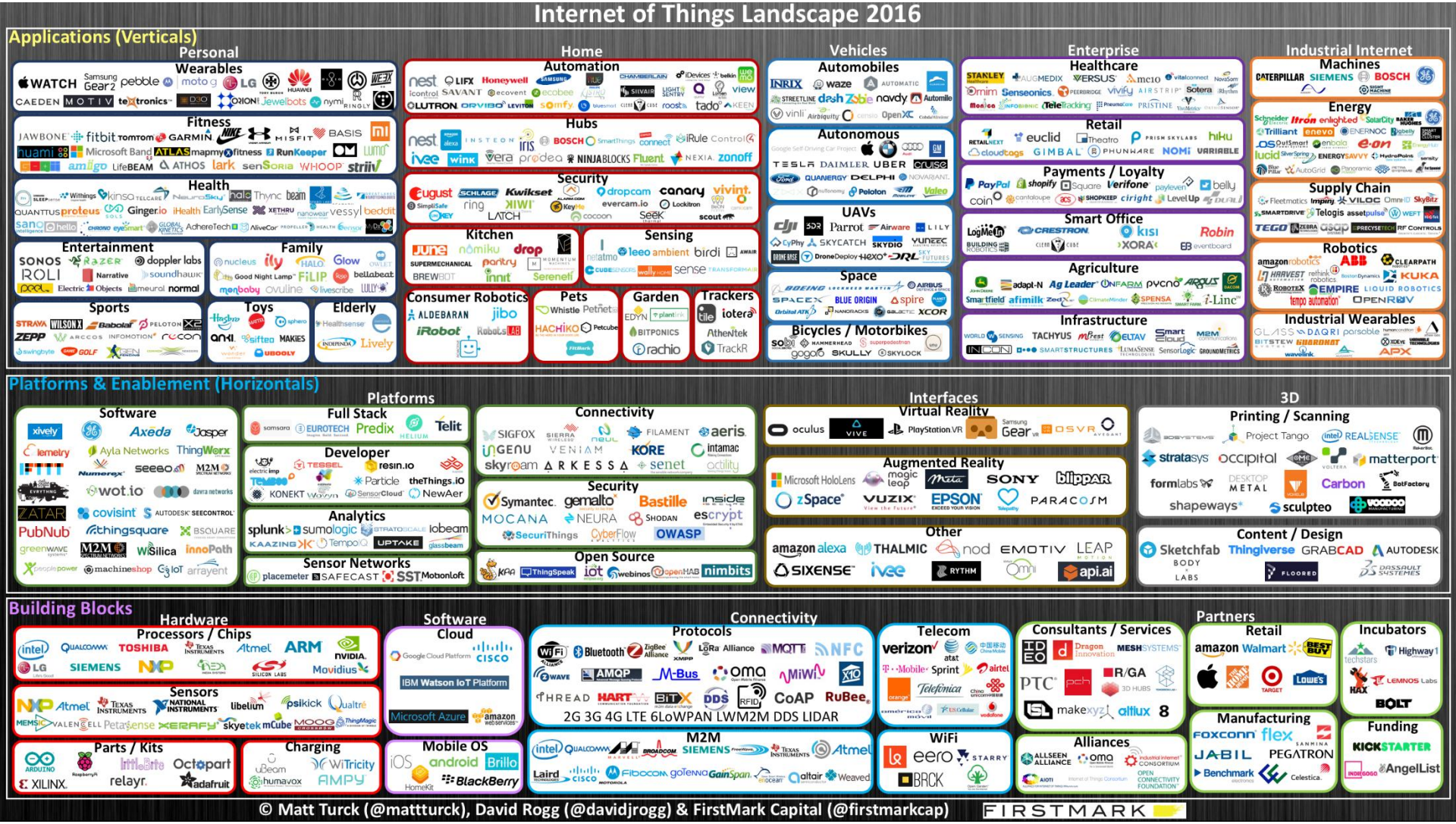
- Les objets connectés sont déjà partout
  - 7 milliards d'objets connectés à l'heure actuelle
  - 20 milliards en 2020 !

- Les applications de ces objets défient l'imagination (exemples à suivre)

Les objets connectés et l'IoT



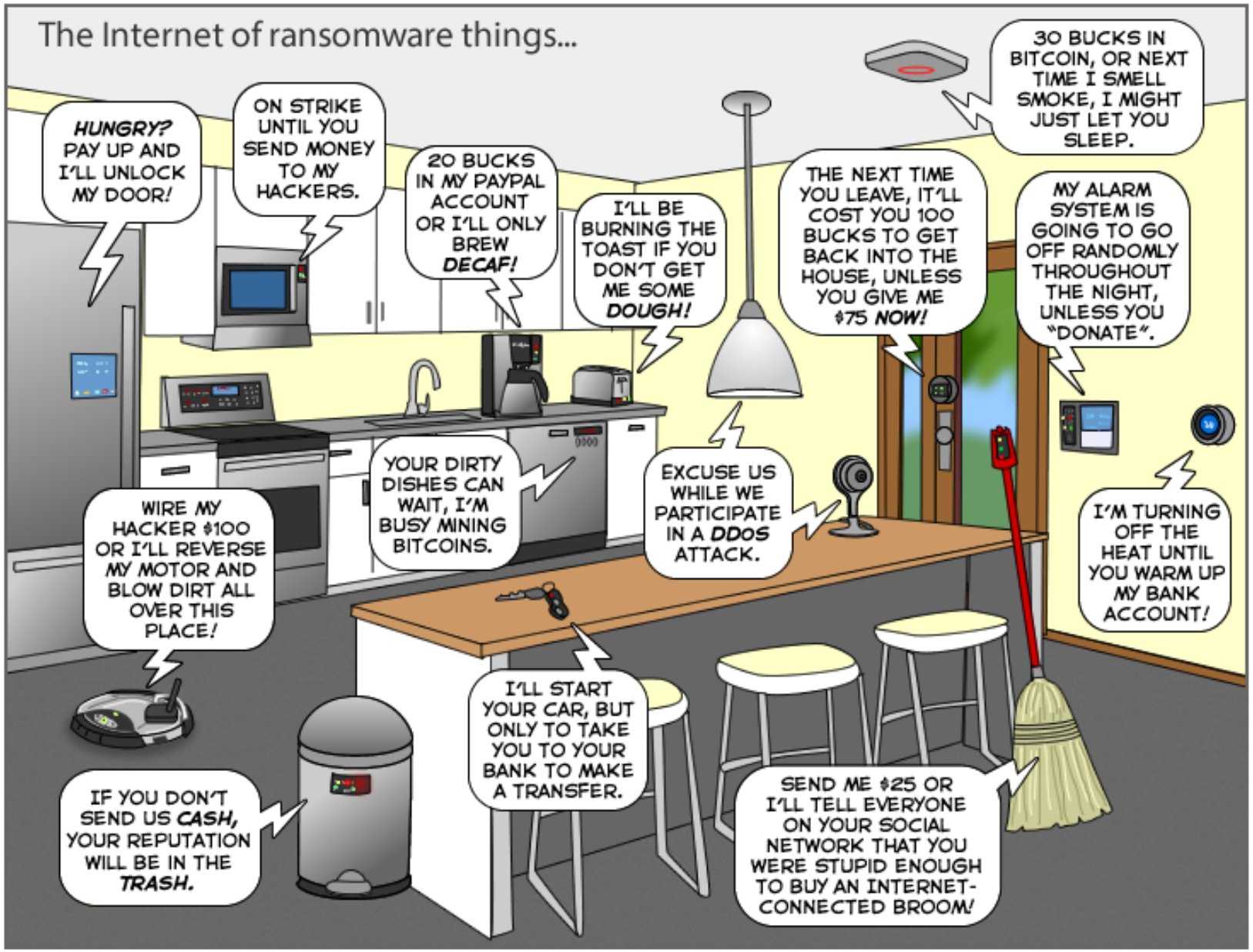
Un paysage gigantesque



La sécurité des objets connectés

- Principales attaques sur les objets connectés
  - Piratage de frigos (envoi de spam)
  - Piratage de serrures connectées et d'éclairage connecté
  - Installation d'application sur télévision connectée et connexion à la Webcam intégrée
  - Piratage de voitures (ex: Jeep)
    - Ouverture de portières
    - Modification de comportements (freins, moteur, …)
  - Attaques sur des pacemakers et des pompes à insuline
    - Le vice-Président américain a fait modifier le sien !
  - Piratage de caméras vidéos (cf plus loin)

La sécurité des objets connectés



La sécurité des objets connectés dans la ville

A Lille aussi…

La sécurité des objets connectés dans le domaine de la santé, un vrai problème…

Hack des pompes à insuline, des pacemakers

Insulin pumps [edit]

At the McAfee FOCUS 11 conference in October 2011 in Las Vegas, while working for McAfee Security, Jack first demonstrated the wireless hacking of insulin pumps, one worn by a diabetic friend and another of the same model on a bench set up for demonstration. Interfacing with the pumps with a high-gain antenna, he obtained complete control of the pumps without any prior knowledge of their serial numbers, up to being able to cause the demonstration pump to repeatedly deliver its maximum dose of 25 units until its entire reservoir of 300 units was depleted, amounting to many times a lethal dose if delivered to a typical patient.[10]

At the RSA Security Conference in San Francisco in February 2012, using a transparent mannequin he demonstrated that he could wirelessly hack the insulin pump from a distance of up to 90 metres using the high-gain antenna.[11]

Pacemakers [edit]

In 2012 Jack demonstrated the ability to assassinate a victim by hacking their pacemaker. This scenario was first explored in fiction on the TV series *Homeland*. In his blog post "Broken Hearts", Jack wrote that the hack was even easier than portrayed: "TV is so ridiculous! You don't need a serial number!"[12] Jack demonstrated delivering such a deadly electric shock live at the 2012 BreakPoint security conference in Melbourne.[4]

In the game Watch_Dogs, a similar hack is shown by black hat Aiden Pearce in killing one of the main antagonists.

Heart implants [edit]

TECHNOLOGY NEWS | Tue Oct 4, 2016 | 3:58pm EDT

J&J warns diabetic patients: Insulin pump vulnerable to hacking

La sécurité des objets connectés en question

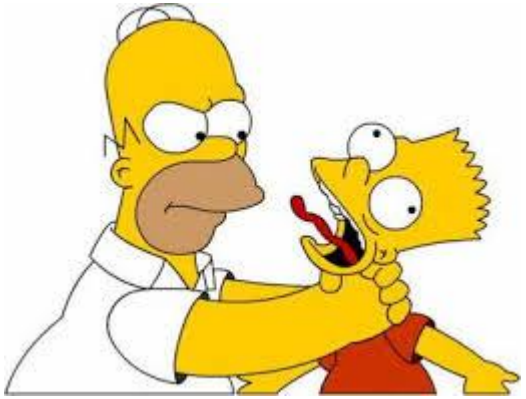
Souvent, de la part des constructeurs, il n'y a pas ou peu de « security by design ».
Les analyses de risques sont négligées ou inexistantes.

La prise de conscience du risque potentiel est tardive.

Pour toutes ces raisons il est compliqué de corriger a posteriori les failles.
Cela ouvre des brèches géantes en matière de sécurité qui sont exploitées par les script kiddies et les cyber criminels.

Le médical, et demain ?

Possibilité de pirater la prothèse de cette jeune femme ?
Avec quelles conséquences ?



A contrario, parfois il n’y a pas de besoin de sécurité et on peut déployer assez vite

Lecteur Mobile Autonome

Testé en remplacement d’un smartphone pour le personnel étranger ou analphabète : une réussite POC avec déploiement dans la foulée

Badgeuse murale :

WIFI (expressif ESP8244) :
802.11 b/g/n
Wifi 2.4Ghz
WPA/WPA2
Température d'utilisation : -40°C à +125°C

GPRS (Ublox SARAH-G350) :
QuadBand : GSM-900- GSM-1800, GSM-850, GSM-1900
Basse consommation < 1mA en veille avancée, <5mA en veille normale
Température de fonctionnement : –40° C to 85° C

RFID :
Lecteur RFID HF (13,56MHz)
Lecture à 15 cms

GPS (Max M8M) en option :

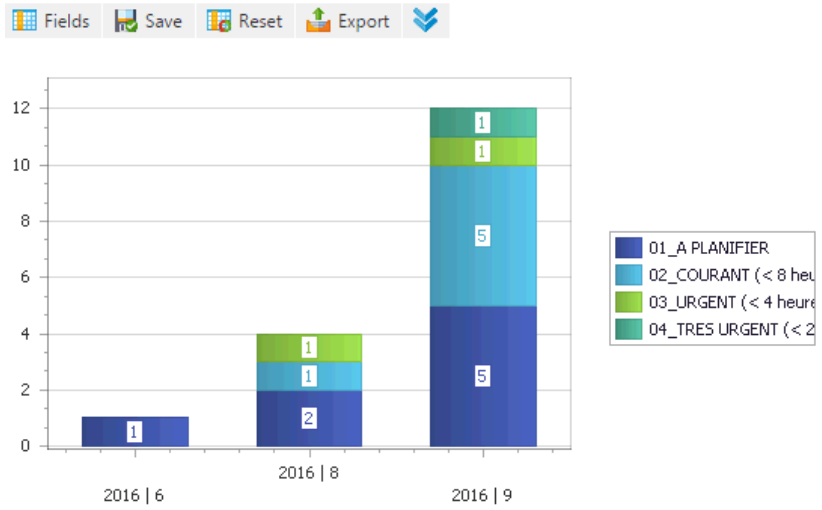
4 GNSS (GPS *(américain)*, Galileo *(europe)*, Glonass *(russe)*, Beidou *(chinois)*)
Forte sensibilité : -167 dBm
Température de fonctionnement : –40° C to 85° C

Mémoire de 2Mo pour stocker les tags (environ 100000) en mode hors connexion
5 Boutons personnalisables
Batterie 1200MA/h pour une autonomie de 6h de lecture continue de tag
Poids: 70 grammes
Dimensions : 11,6 cm x 5,2 cm x 1,4 cm

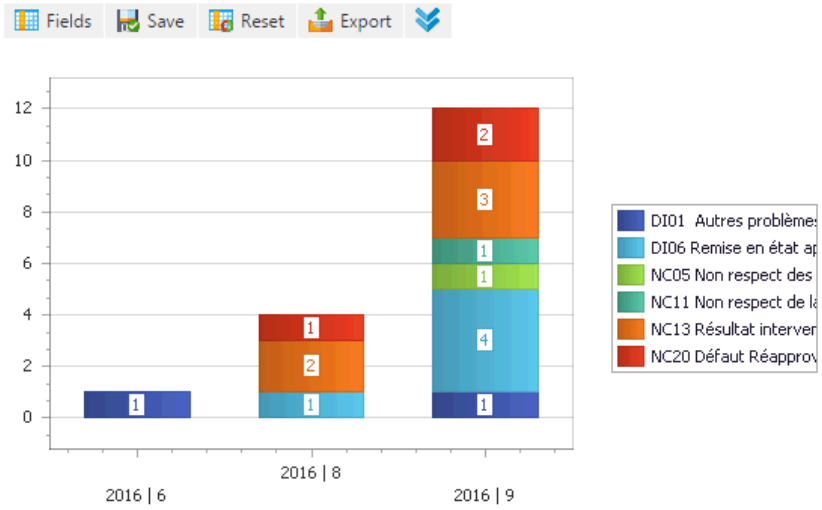
A contrario, parfois il n’y a pas de besoin de sécurité et on peut déployer assez vite

Les enjeux de sécurité sont très faibles, les bénéfices en termes d’exploitation sont élevés, l’impact en cas de piratage est ridicule => donc mise en œuvre immédiate

Demandes d'interventions par priorité (nettoyage / picking / consommables)



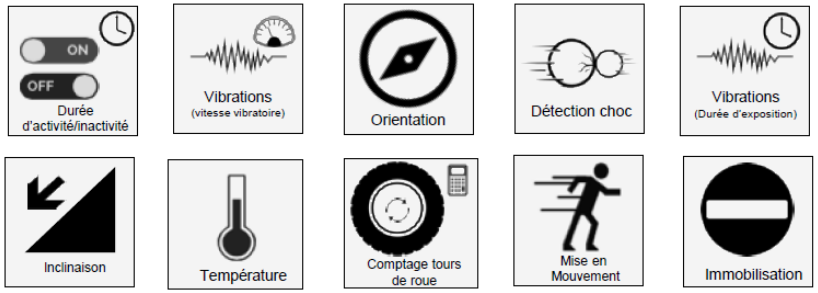
Demandes d'interventions par problème (nettoyage / picking / consommables)



A contrario, parfois il n'y a pas de besoin de sécurité et on peut déployer assez vite

Exemple de capteur multifonction pour des domaines d'applications variés : les limites sont celles de votre imagination !
Et parfois la sécurité est VRAIMENT la dernière des priorités : ex : capteur de localisation d'un chariot aéroport ou ventre commercial : pas de bidirectionnalité de dialogue réseau : très peu de risque.

11
Fonctionnalités



IP 65

Taille : **44 x 20 x 23 mm**
Volume : **20 cm^3**

- **Encombrement minimum**
- **Fixation multiples**

Parfois on déploie sans avoir bien évalué le besoin de sécurité ?

ENTREPRISES ET MARCHÉS

EQUIPEMENT

Nilfisk se lance dans la robotisation

| 25 octobre 2016 |

(DR)

The Horizon program : c'est le nom donné par Nilfisk à son nouveau plan stratégique de développement de produits. Avec ce programme, présenté le 4 octobre dernier, le fabricant danois se lance officiellement dans la course à la robotisation en partenariat avec Carnergie Robotocs, l'un des spécialistes américains des capteurs et des logiciels embarqués.

La collaboration entre les deux sociétés vise le développement d'une série de nouvelles solutions de nettoyage autonomes et « intelligentes ». « Avec The Horizon program , nous nous engageons dans un programme stratégique et à long terme de solutions autonomes et connectées s'appuyant sur la technologie la plus sophistiquée qui va complètement redéfinir la façon dont nous envisageons la productivité et le coût total de possession », a déclaré Jonas Persson, président et CEO du groupe Nilfisk. Le lancement du premier robot est annoncé pour le printemps 2017. Il s'agit d'une autolaveuse conçue pour travailler en mode manuel ou complètement automatique. Elle sera présentée en avant-première lors de l'édition américaine d'ISSA-Interclean (du 25 au 28 octobre à Chicago).

Possibilité de pirater l'auto-laveuse et de l'envoyer dans le décor ?

Quid des responsabilités ?
Quid du travail dans des zones où circule le public ?

A contrario : avantage en terme de pénibilité au travail pour les opérateurs: vibrations, gestes et postures.

Quelques attaques récentes

- DDoS sur OVH en France
- DDoS sur des sites américains
- Ver sur les ampoules connectées Philips

Quelques attaques récentes

DDoS sur OVH

- Attaques DDoS sur certains clients d'OVH du 18 au 23 septembre 2016
- Pointe à 1,15 Tb/s de trafic malveillant atteint le 20 septembre
  - Débit encore jamais vu !
- Source: botnet de caméras de sécurité (145 000 caméras infectées)
  - Chacune peut envoyer entre 1 et 30 Mbps de trafic malveillant vers la cible !
  - Pas besoin d'exploiter un mécanisme de réflexion/amplification comme pour les attaques UDP ou DNS

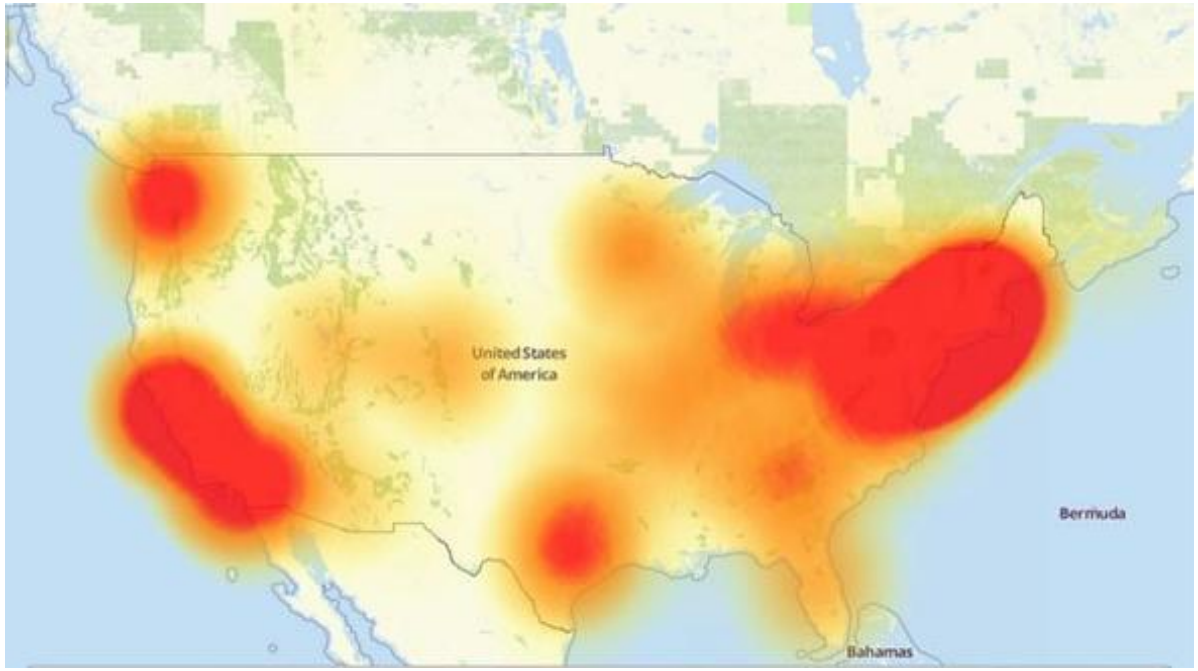
DDoS sur OVH

- Compromission des caméras
  - Botnet « Mirai »
  - Scanne le port TCP 2323 sur Internet et identifie les objets connectés
  - Utilise les comptes et mots de passe par défaut (60 mots de passe faibles ou par défaut sont testés par le malware)
  - Installation du malware
  - Pilotage à distance des caméras (C&C)
  - Autres équipements compromis: DVR, NAS, routeurs/box, Raspberry Pi, …
  - Code source de Mirai « leaké » (publié) sur: https://github.com/jgamblin/Mirai-Source-Code

- Conséquences
  - OVH a bien résisté grâce à ses connexions à de multiples opérateurs
  - Le constructeur chinois des caméras a rappelé plusieurs millions de caméras
    - Hangzhou Xiongmai Technology: http://www.xiongmaitech.com/en

DDoS sur des sites américains

- Le 21/10/2016, les sites Twitter, Spotify, PayPal, Netflix, AirBnb, PayPal, PlayStation Network, etc… hébergés sur la côte est et la côte ouest des USA deviennent injoignables pendant une dizaine d'heures



DDoS sur des sites américains

- Attaque indirecte:
  - Attaque DDoS sur le fournisseur de services DNS « Dyn »
  - Conséquence: les clients de Dyn deviennent inaccessibles sur Internet
  - Une soixantaine de sites sont impactés: https://fr.wikipedia.org/wiki/Cyberattaque_de_2016_contre_Dyn
  - Quelques dysfonctionnements ponctuels en Europe

- Utilisation du botnet Mirai à nouveau
  - Jusqu'à 500 000 objets piratés
  - Plus de 1 Tb/s de débit

Ver sur des ampoules connectées

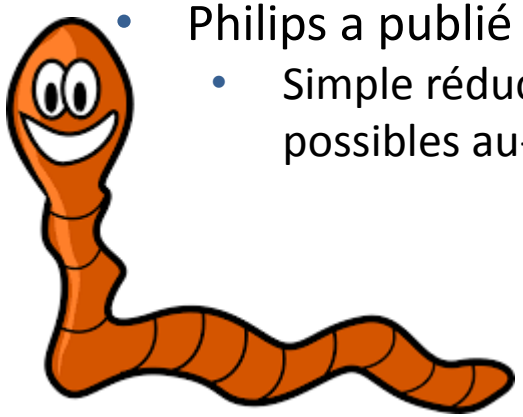
- Ampoules connectée Philips Hue
- Des chercheurs ont montré qu'il est possible d'infecter une ampoule à 400 m de distance et d'y insérer un malware qui va se propager d'ampoule en ampoule
- Propagation autonome en mode « ver »
- Masse critique de 15 000 ampoules suffisante pour infecter automatiquement une grande ville entière

- Conséquences:
  - Brouillage des réseaux en 2,4 GHz (Wifi, ZigBee, …)
  - Extinction de l'éclairage
  - Allumage de toutes les ampoules (pics/écarts de consommation)
  - Clignotement ➔ crises d'épilepsie ! ☺

Ver sur des ampoules connectées

- Détails de l'attaque
  - Exploitation d'une faille dans l'implémentation du protocole ZigBee Light Link (ZLL)
  - Extraction de la clé secrète identique dans toutes les ampoules
    - Par différences de consommation
  - Mise à jour du firmware signé par cette clé
  - Attaque des autres ampoules situées en proximité
  - Possibilité de lancer l'attaque depuis une voiture ou un drone !

- Philips a publié un patch en octobre 2016
  - Simple réduction de l'impact: les connexions malveillantes ne sont plus possibles au-delà d'1 m de distance



Mesures de sécurisation

- Protéger physiquement l'accès aux les objets connectés
- Segmentation réseau: les objets ne doivent pas être directement accessibles sur Internet
  - Notamment les interfaces d'administration
- Chiffrement et authentification réciproque des connexions
  - Utiliser des protocoles reconnus et réputés sûrs (TLS)
  - Avec vérification du certificat du serveur ! Sinon, attaque « man in the middle » possible
  - Empêcher le rejeu
- Modifier tous les mots de passe par défaut
  - Notamment les interfaces d'administration et les interfaces « dans le Cloud »
- Appliquer les mises à jour logicielles/de firmwares diffusées par les éditeurs
- Gérer le cycle de vie de ses objets connectés (enrôlement ➔ destruction)
- Chiffrer les données sur les équipements et dans le Cloud

Mesures de sécurisation

- Points durs
  - Mauvaise implémentation des protocoles (ex. des ampoules connectées)
  - Failles intrinsèques aux protocoles (Wifi, BLE, ZigBee, …)
    - Déconnexions des équipements du réseau radio
    - Consommation élevée et épuisement de la batterie
  - Accès physique aux équipements
    - Attaques « hardware »

- Points positifs
  - Certains constructeurs ont bien compris les risques d'attaques sur leurs objets connectés
  - Ils commencent à prendre en compte les mesures de sécurité à intégrer dans leurs produits

Conclusion

- Les objets connectés sont déjà partout
- Leur sécurité est encore insuffisante
- Les impacts dans le monde physique ou numérique des attaques sur les objets connectés devient non négligeable
- Il y a encore beaucoup de travail de sécurisation à faire pour éviter… le début du soulèvement des machines ? ;-)

Questions ?