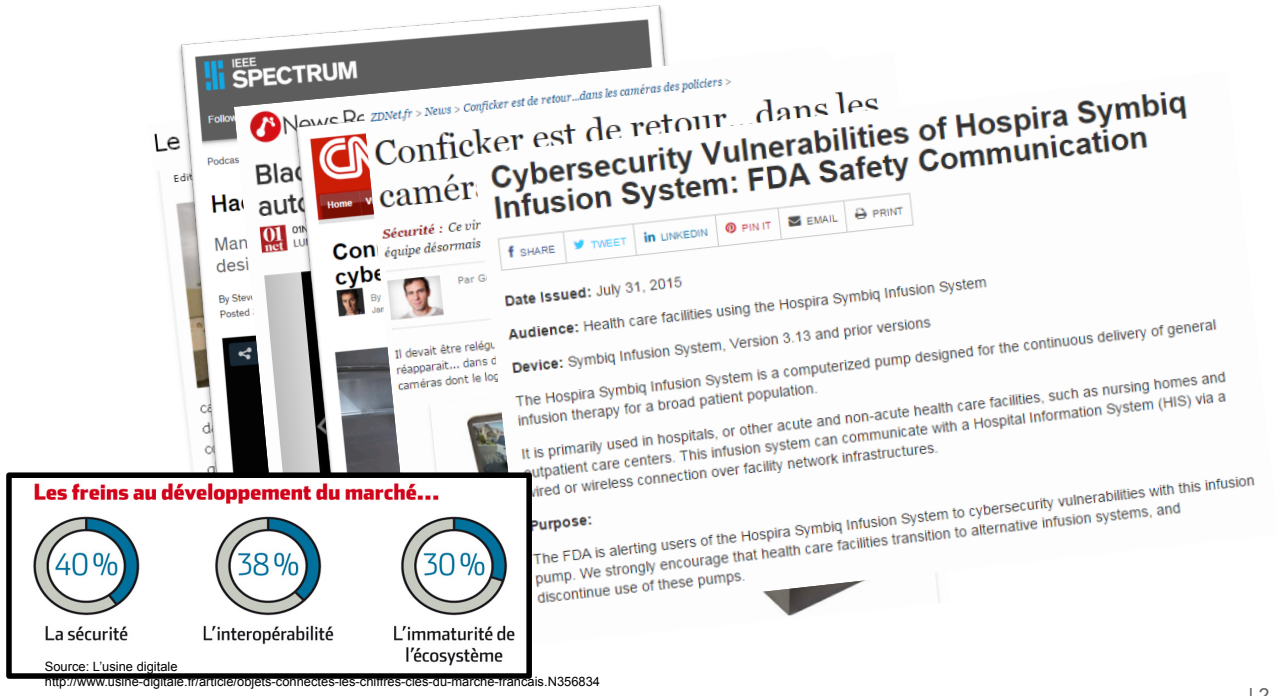
leti
cea tech

Cybersecurity Institute
Univ. Grenoble Alpes

ENJEUX DE SÉCURITÉ POUR LES NŒUDS IOT

15 Mai 2018

Jacques FOURNIER, PhD, HDR



Source: L'usine digitale
http://www.usine-digitale.fr/article/objets-connectes-les-chiffres-cles-du-marche-francais.N356834

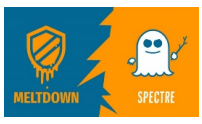
Adi Shamir **fait 15 predictions pour les 15 prochaines années dans le 'keynote' anniversaire de "Financial Cryptography 2016" :**

1. *Cybersecurity is terrible, and will get worse.*
2. *The Internet of Things will be a security disaster.*
3. *…*




L'objet de plus en plus au cœur des attaques

Dernière/Première Ligne de Défense | **CŒUR(s) de tout système**

« Dématérialisation » de la notion de Risques

La Sécurité, c'est complexe…

Les technologies actuelles, pas adaptées…

La Sécurité : à la traîne…

Schémas de ceritifs/valids : pas adaptés

Pourquoi ?

- **Utilisations ludiques**
- **Privilégie le côté pratique/fun**
- **Modèles économiques à court terme**

« Dématérialisation » de la notion de Risques

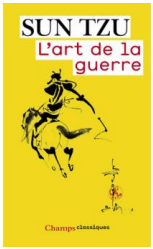
Enjeux

- Modèles d'analyses de risques adaptées
- Modèles de gouvernances industrielles adaptées à la gestion de crise « cyber » et à l'adoption de technos de sécurités
- Politiques de gouvernances et législations adaptées
- Nouveaux modèles économiques?

Pourquoi ?

La Sécurité, c'est complexe…

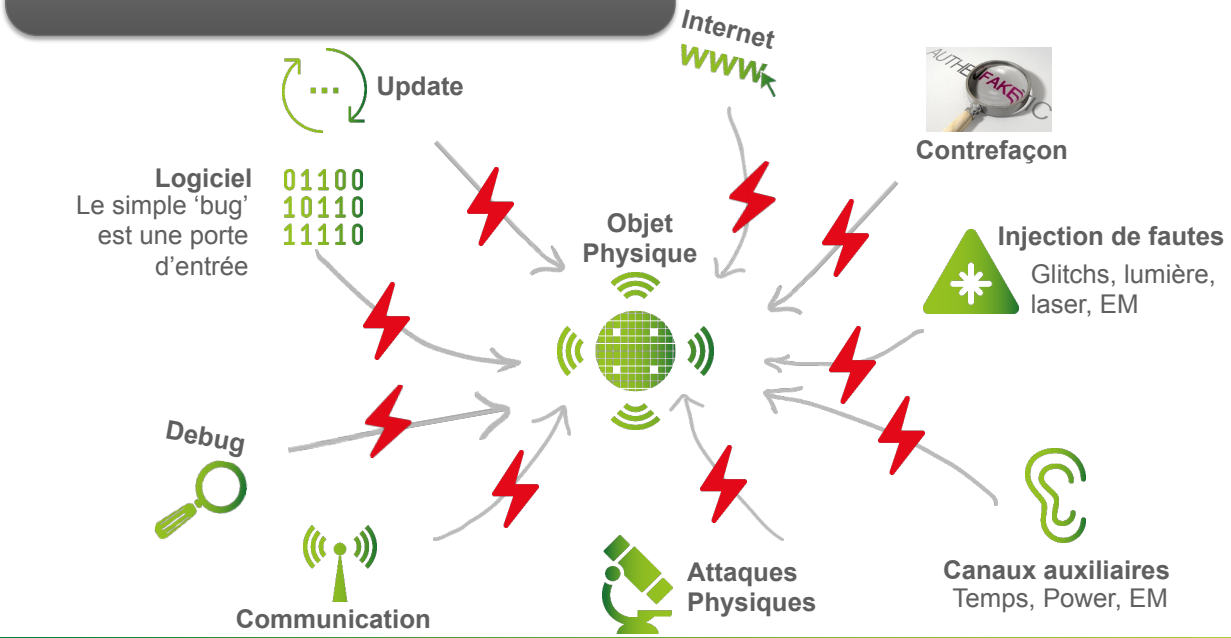
- **Des maths, des maths & des maths…**
- **Les systèmes sont complexes**
- **Intègre des multi-compétences techniques**
  - Electronique – Informatique
- **La sécurité c'est L'Art de la Guerre !**



Enjeux

- Formations adaptées et surtout pluridiscplinaires
- Convergence entre
  - Sureté – Résilience – Sécurité
  - Automatisme – Informatique
  - Choix technos *versus* Aspects légaux/législatifs/sociétaux
- Solutions techniques les plus transparentes possibles
- Solutions « adaptables »
  - Mises à jour sécurisées

La Sécurité de l'objet, c'est complexe…



Pourquoi ?

Nous faisons les solutions de demain avec les technologies d'hier…

- Archi de proc, crypto, protocoles IP

Les technologies actuelles : pas adaptées

Enjeux

- Nouvelles technos:
  - Processeurs intrinsèquement sécurisés,
  - nouvelles cryptos,
  - Sécurisations intrinsèques de composants (PUFs…)
  - Générateurs de nombre aléatoires « non techno dépendantes »
  - Processus / protocoles résilients et robustes
  - Sécurisation des mécanismes d'accélérations, de gestions de l'énergie etc

Pourquoi ?

- **Course contre les performances**
- **Course contre l' Ordinateur Quantique**
- **Course contre l' IA**

La Sécurité : à la traîne…

Enjeux

- Formations adaptées et surtout pluridiscplinaires
- Enjeux forts :
  - Sureté – Sécurité
  - Automatisme – Informatique
  - Choix technos *en adéquation avec* Aspects légaux/législatifs/sociétaux
- Remettre la sécurité au centre (ou au début) de nos cycles de vie et productions des objets.

Pourquoi ?

- **Schémas CC adaptés pour un marché « de niche »**
- **Autres schémas pas satisfaisants?**

Schémas de ceritifs/valids : pas adaptés

Enjeux

- Schémas économiquement viables (besoins industriels et besoins des utilisateurs)
- Quid des travaux actuels de l'ENISA?
- Schémas par secteurs d'activités?

Quid de l'évolution du modèle d'attaquant?