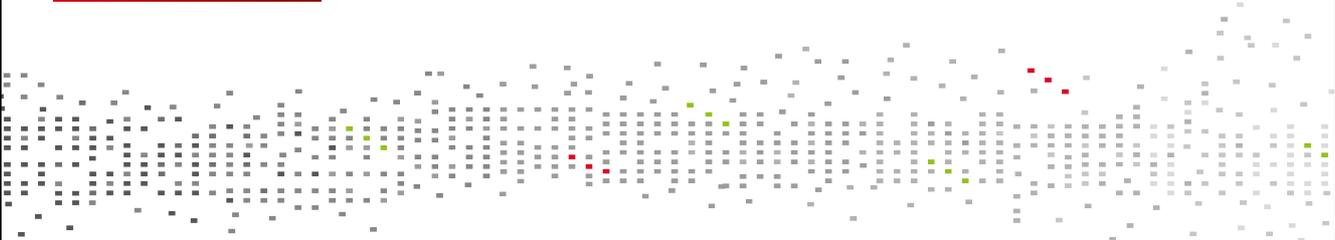




Cybersecurity Institute
Univ. Grenoble Alpes



ENJEUX DE SÉCURITÉ POUR LES NŒUDS IOT

15 Mai 2018

Jacques FOURNIER, PhD, HDR



Les freins au développement du marché...

40%	38%	30%
La sécurité	L'interopérabilité	L'immaturité de l'écosystème

Source: L'usine digitale
<http://www.usine-digitale.fr/articler/objets-connectes-les-chiffres-clés-du-marché-français.N356834>

IEEE SPECTRUM
 Conficker est de retour... dans les caméras
 Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication

Date Issued: July 31, 2015
Audience: Health care facilities using the Hospira Symbiq Infusion System
Device: Symbiq Infusion System, Version 3.13 and prior versions

The Hospira Symbiq Infusion System is a computerized pump designed for the continuous delivery of general infusion therapy for a broad patient population. It is primarily used in hospitals, or other acute and non-acute health care facilities, such as nursing homes and outpatient care centers. This infusion system can communicate with a Hospital Information System (HIS) via a wired or wireless connection over facility network infrastructures.

Purpose:
 The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump. We strongly encourage that health care facilities transition to alternative infusion systems, and discontinue use of these pumps.

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. ...

| 3



L'objet de plus en plus au cœur des attaques

Dernière/Première Ligne de Défense

CŒUR(s) de tout système



| 4

POURQUOI,
POURQUOI,
POURQUOI ?



« Dématérialisation » de la notion de Risques

La Sécurité, c'est complexe...

Les technologies actuelles, pas adaptées...

La Sécurité : à la traîne...

Schémas de certifs/valids : pas adaptés

| 5

Pourquoi ?

« Dématérialisation » de la notion de Risques

Utilisations ludiques

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



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?

| 6

Pourquoi ?

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 !

La Sécurité, c'est complexe...

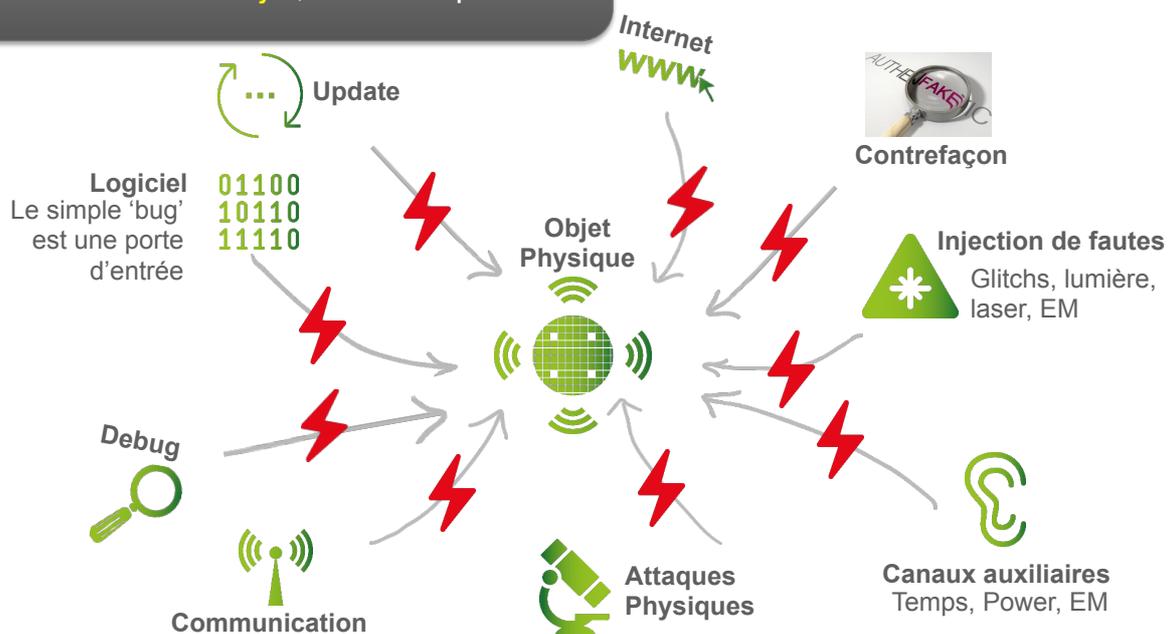
Enjeux

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



17

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



18

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'accélération, de gestions de l'énergie etc

| 9

Pourquoi.?

Course contre les performances

- Course contre l' Ordinateur Quantique
- Course contre l' IA

La Sécurité : à la traîne...

Enjeux

- Formations adaptées et surtout pluridisciplinaires
- Enjeux forts :
 - Sureté – Sécurité
 - Automatisation – 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.

| 10

Pourquoi.?

Schémas CC adaptés pour un marché « de niche »

- Autres schémas pas satisfaisants?

Schémas de certifs/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?

| 11

Quid de l'évolution du modèle d'attaquant?



| 12