La sécurité à l’ère des objets connectés

Comment s’y prendre quand on est une PME qui en conçoit ?

Qui sommes nous ?

OPALE SECURITY créée en 2008

- Conseil en sécurité des SI
- Conseil en sécurité des objets connectés
- Conception d'outil d'audit de sécurité IoT
- Centre de formation cybersécurité + IoT sécurisé

Notre offre de service (IoT Security)

- Test d'intrusion software & Hardware
- Audit
- Assistance à la conception sécurisée
- Gestion des risques
- Mise en place de stratégie de sécurité (PSSI, SDLC)
- Formation & sensibilisation

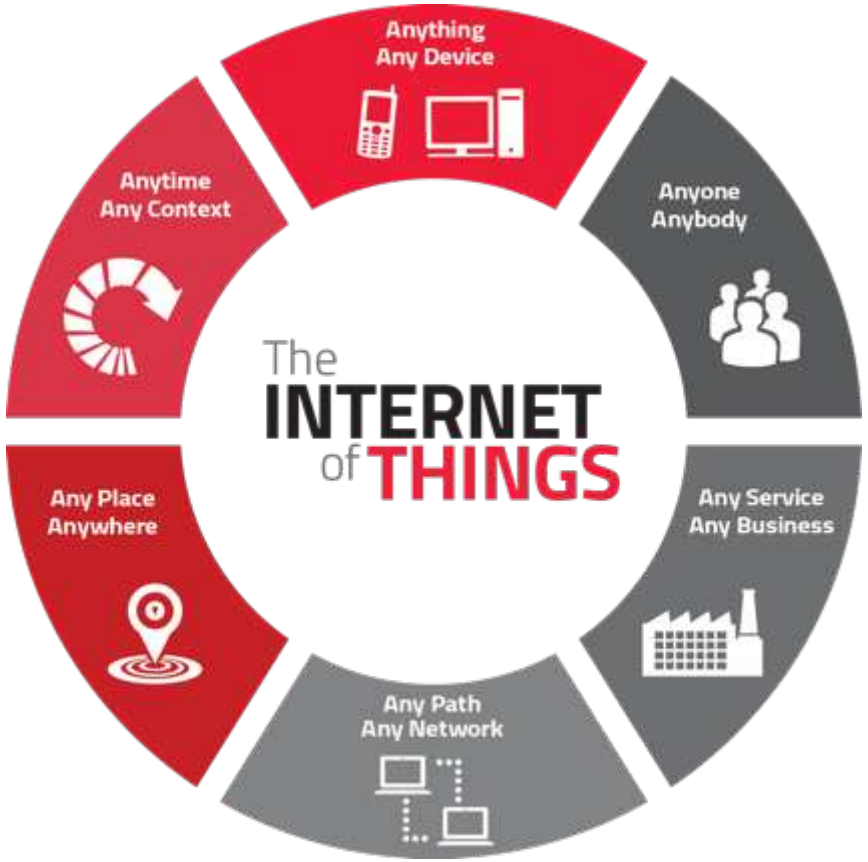
Yann ALLAIN (CEO & Consultant)

- 20 ans d'expérience
- Sécurité IT et IoT
- Ancien responsable de la sécurité applicative du groupe ACCOR
- Ingénieur en électronique
- Blackhat, HITB Speaker
- Hardware Hacking Trainer

IoT& Hacking : de quoi parle-t-on ?

D'un point de vue offensif, l'internet des objets c'est :

- Des systèmes électroniques
    - qui sont plus ou moins directement exposés aux menaces d'Internet (comme le SI)
    - Dont les capacités techniques sont limitées par rapport au PC traditionnel
    - Mais qui stockent ou transmettent des données parfois sensibles, confidentielles, personnelles…
    - Sans discontinuité entre les mondes **physiques et virtuels**
    - **Dont le niveau de sécurité est parfois … insatisfaisant**
    - **C'est un domaine ou les risques et le niveau de la menace sont (souvent) sous estimés.**



IoT= un écosystème complet

IoT devices

HF communications (ISM Band) + Wifi + 3G-5G , Bluetooth, Sigfox, Lora etc..

Classical wired connections

Central servers, user Interface, API, backoffice etc.

Conseil 1 : C'est la chaine complète qu'il faut sécuriser !

IoT = Domaine où les risques réels existent

Conseil 2 : Ça n'arrive pas qu'aux autres !

IoT = Nouvelle porte d'entrée pour les pirates … et les autres!

US intelligence chief: the Internet of Things will be used to spy and hack

By: Graham Cluley | comment : 1 | February 15, 2016 | Posted in: Industry News

opportunities for our own intelligence collectors.

Internet of Things (IoT). "Smart" devices incorporated into the electric grid, vehicles—including autonomous vehicles—and household appliances are improving efficiency, energy conservation, and convenience. However, security industry analysts have demonstrated that many of these new systems can threaten data privacy, data integrity, or continuity of services. In the future, intelligence services might use the IoT for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials.

Artificial Intelligence (AI). AI ranges from "Narrow AI" systems, which seek to execute specialized tasks, such as speech recognition, to "General AI" systems—perhaps still decades away—which aim to

Conseil 3 : Même si vos IoT ne sont pas sensibles ils seront sans doute utilisés…de facon malveillante !

IoT = Une surface d'attaque sans fin?

marasawr @marasawr - 9 févr.

In Oct @DARPA said IoT is proliferating attack surfaces faster than *humans* can secure them. #LiabilityOrGTFO

Schneier on Security

Blog | Newsletter | Books | Essays | News | Speaking | Crypto

← Security vs. Surveillance | Tracking Anonymous Web Users →

The Internet of Things Will Be the World's Biggest Robot

KIM ZETTER SECURITY 02.09.16 10:40 AM

HOW TO HACK THE POWER GRID THROUGH HOME AIR CONDITIONERS

Conseil 4 : la prolifération des technologies différentes ne rend pas facile la sécurisation : Soyons donc préparer aux mieux à de nouveaux scénarios de menace !

Quelques exemples

Des malwares dans votre carte réseau, les voitures, les pacemakers, les pompes à insulines, les DAB, les automates industriels, les smartmeter…etc

"ATM Jackpotting" Blackhat USA Aug 2010

Retour d’expérience

- Issue de nos 100 dernières missions « sécurité IoT »

- Concernant
  - L’assistance à la conception sécurisée d’écosystemes d’objets connectés
  - L’audit / Test d’intrusion IoT

- Impacts des objets (parfois TRES gros !) qui roulent, volent, de nature industriels, des Box Home office, des objets du quotidien etc…

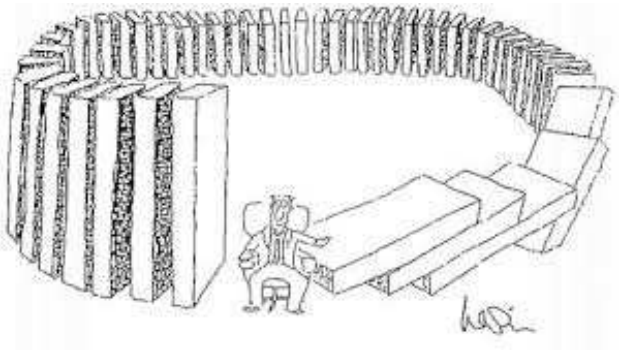
- Que faut il retenir?

Constat 1
La sécurisation au second plan

- Seules 38% se focalisent sur la sécurité dès le début de la phase de développement du produit

- **Maturité de la filière?**

Les conséquences ?



- 82% des objets connectés ne chiffrent pas leurs communications sur les réseaux
- 65% n'offrent pas une interface Web suffisamment sécurisée
- 80% posent des problèmes de confidentialité des données
- 57% des objets connectés testés ne sécurisent pas le téléchargement des *updates*
- 50 % des industriels ne protègent pas les couches électroniques (Chip, Jtag, etc…)
- 90 % des industriels / Ingénieurs ne connaissent pas les menaces réelles et ne savent pas évaluer la robustesse de leur propre produit.
- 84 % des industriels n'évaluent jamais la sécurité de leur produit
- 90 % des consultants en sécurité SI ne sont pas formés à la sécurisation des IoT !!!

(Source : retour de nos missions IoT chez Opale Security)

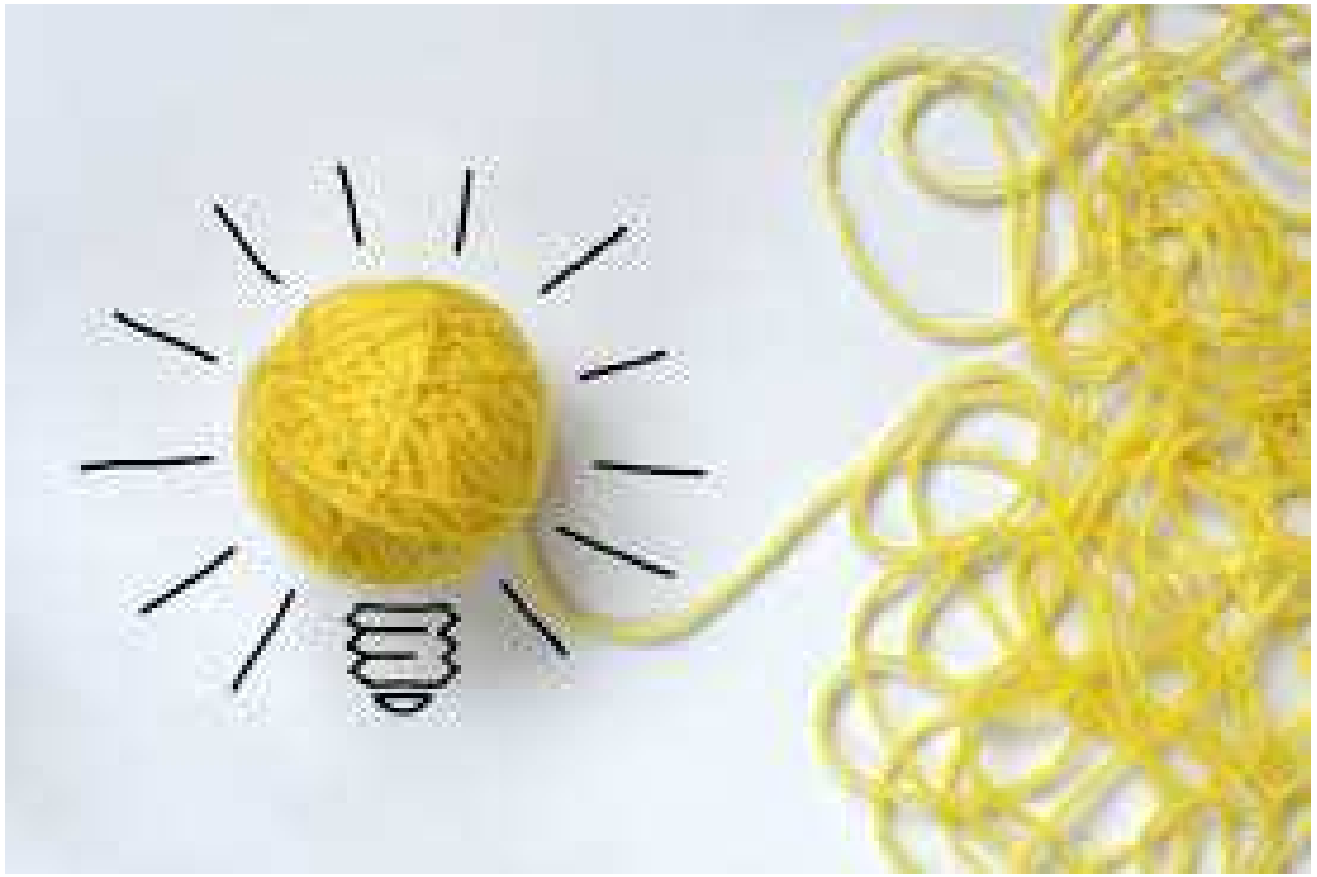
Que faire?

Quand tout deviendra peu ou prou un objet connecté !

Pourquoi Manitowoc connecte ses grues

27/01/2016

Par où prendre cette « pelote de laine ? »



Synthèse de certains risques et comment les réduire

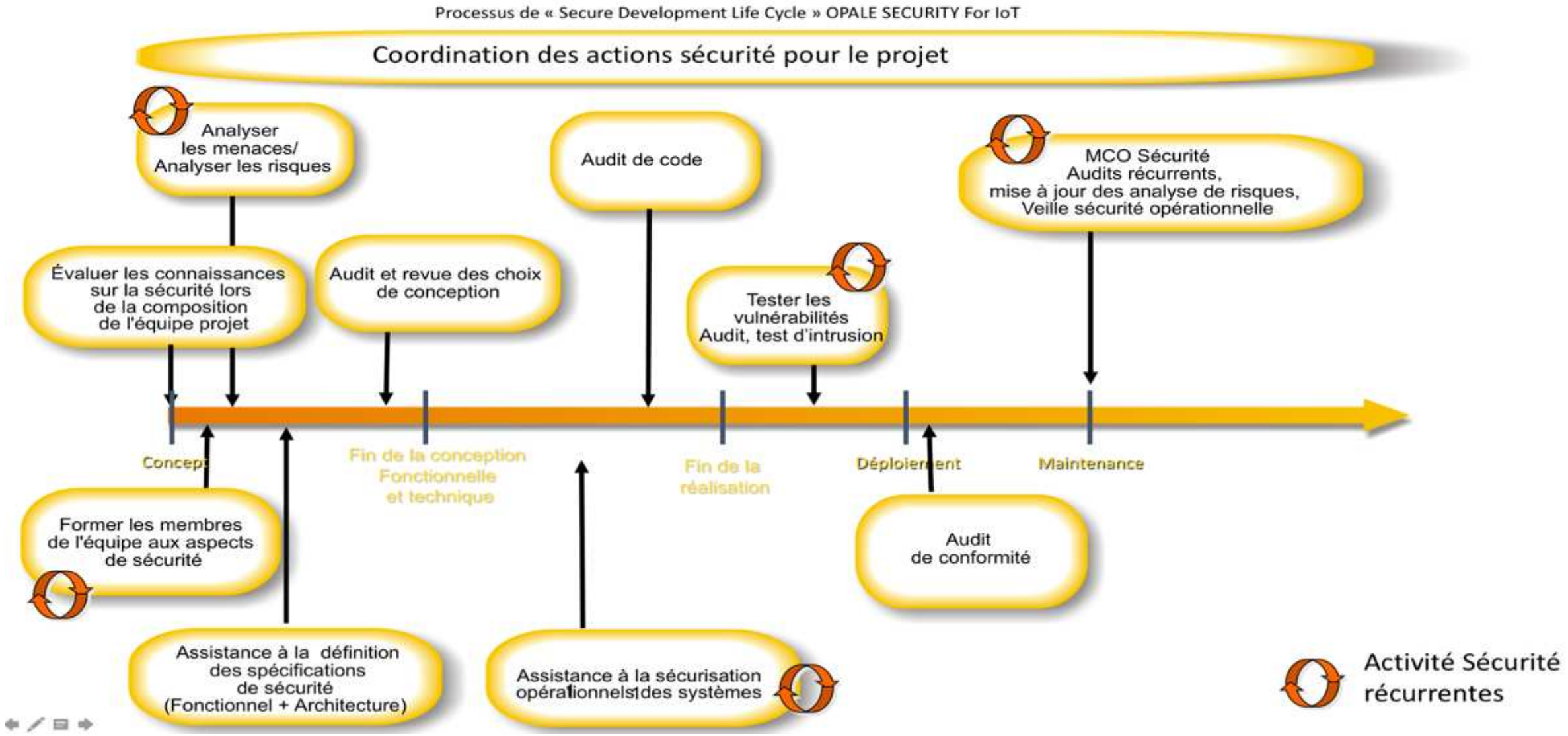
Une faille peut avoir un impact de sécurité significatif

- **Risque d'intrusion** sur l'objet
- **Risque d'atteinte à la confidentialité** ou l'intégrité des données traitées par l'objet
- **Risque de perte de la disponibilité** ou de l'intégrité du processus auquel est « accroché » l'objet (Chaine logistique, outil médical) etc..
- **Risque d'atteinte à la propriété intellectuelle** (le firmware des objets, reverse engeneering)
- **Risque d'attaque par rebond sur les systèmes connectés à l'objet** (Serveur central, autres objets, SI métiers, SI de l'entreprise, bureautique, etc)
- **Risque de perte de conformité** (normes)
- **Risque juridique**, notamment avec la loi CNIL, obligation, sous peine d'amende à diffuser publiquement que vous auriez subit une attaque

Comment agir?

- **Analyser la surface d'attaque** des objets connectés (Analyse d'architecture, comprendre les adhérences de sécurité avec les systèmes tiers inclus)
- **Réaliser un test d'intrusion Hardware** sur les objets pour mesurer leur robustesse à ce type de faiblesses
- **Mettre en place d'un processus de conception sécurisée** (Soft + Hard) qui n'influe en rien sur les coûts ou sur les temps de développement
- **Former les équipes de R&D** à la prise en compte de la sécurisation dès les phases de conception et pendant toute la vie du projet (patch management)
- **Utiliser des outils d'aide à l'audit** de sécurité IoT (hardsploit)
- **Auditer régulièrement** les process, les écosystèmes
- **Maintenir le niveau de sécurité en conditions opérationnelles** dans le temps

Mettre en place un SDLC IoT



Vers un début de solution

Pour les constructeurs:

- Reconnaître l'existence des risques
- Inclure une dimension de sécurité dans le développement & l'utilisation des objets connectés
- Proposer des systèmes de signalement et de correction des vulnérabilités au fur et à mesure de leur détection
- Evaluer la sécurité des produits (Pentest de l'ecosysteme Hardware)

Pour les utilisateurs / entreprises

- Se tenir informer (veille technologique)
- Mettre à jour
- Capacité à anticiper et à réagir aux incidents de sécurité

Conclusion

- On reste à votre disposition (sales mode = on) ⏪
- **IMHO, la connaissance et la maitrise des menaces réelles par vos ingénieurs de conception est une des clés de la réussite de la sécurisation des objets connectés -> Fort besoin en formation !**
- Mais retenez SVP qu'une fonction de sécurité n'est pas forcement une fonction sécurisée

Questions?

- Merci de votre attention

- Pour nous contacter
  - Yann ALLAIN – 06 45 45 33 81 – yann.allain@opale-security.com
  - www.opale-security.com
  - hardsploit.io

- Nos prochaines interventions
  - Conférence Hack In Paris - IoT offensiv for Pentester (Juin 2016)
  - Conférence Captronic Paris (Juin 2016) – IoT & Cybersecurity
  - TRAINING BlackHat – IoT Security audit for pentester- Aout 2016 - Las Vegas