Internet des Objets et sécurité : une mission impossible ?

Damien "virtualabs" Cauquil

Les Matinales de l'embarqué, 15 Mars 2017

Qui suis-je ?

- Responsable R&D et chercheur sénior au CERT-UBIK
- Spécialisé dans la sécurité des solutions connectées
- Conférencier (Hack.lu, Nuit du Hack, Hack in Paris, CCC, DEFCON IoT Village)

Agenda

- Sécurité des objets connectés
  - Anatomie d'une solution connectée
  - Différentes couches de sécurité
  - Synthèse des vulnérabilités les plus courantes
- Nécessité de repenser la sécurité
  - Nouveaux vecteurs d'attaque
  - Environnements inhabituels
  - Traçabilité et journalisation
  - Règlementation et obligations légales
- Conclusion

Sécurité des objets connectés

Sécurité des objets connectés

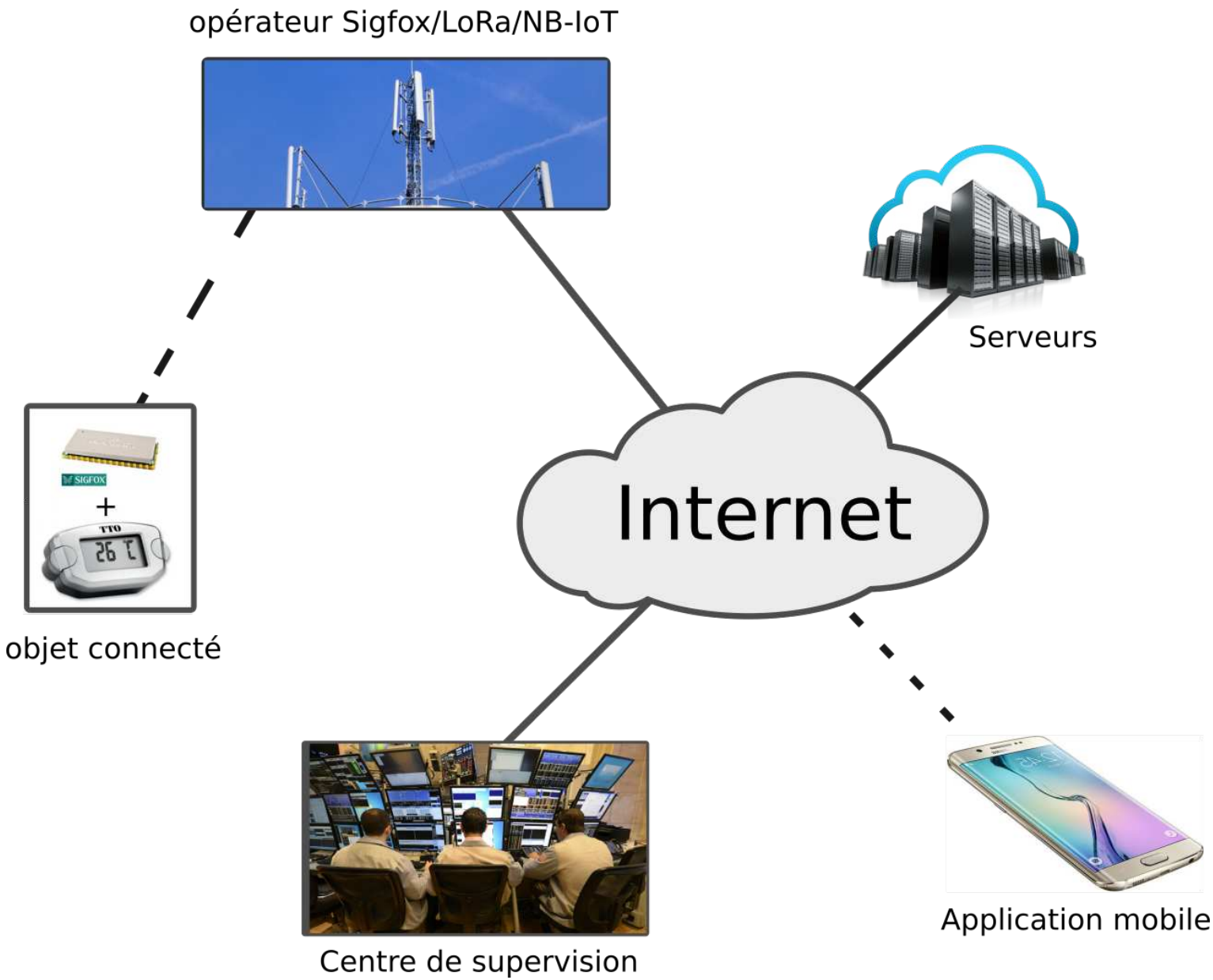
Définitions

Objet connecté : dispositif présent dans le monde réel que l'on a connecté directement ou indirectement à Internet.

Solution connectée : ensemble des dispositifs, technologies de communication, serveurs et applications permettant d'offrir un ou plusieurs services.

Sécurité des objets connectés

Anatomie d'une solution connectée



Sécurité des objets connectés

Anatomie d'un objet connecté

Un objet connecté est constitué :

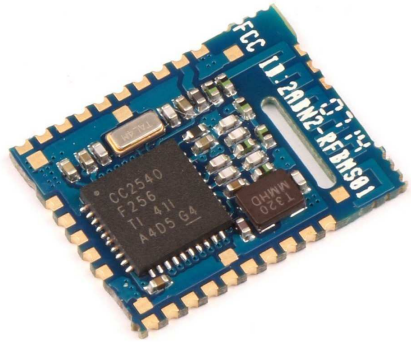
- d'une **base matérielle**, fournissant un système de base ainsi que des périphériques (capteurs, émetteurs, récepteurs, etc.) ;
- d'une **base logicielle** fournissant la logique métier ;
- d'un **moyen de communication** permettant d'échanger des informations avec d'autres dispositifs.

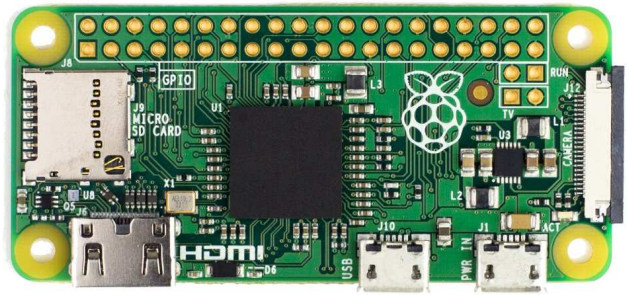
Sécurité des objets connectés

La base matérielle

La base matérielle peut être :

- Un micro-contrôleur ;
- Un *System-on-Chip* ou SoC ;
- Un micro-ordinateur de poche ;



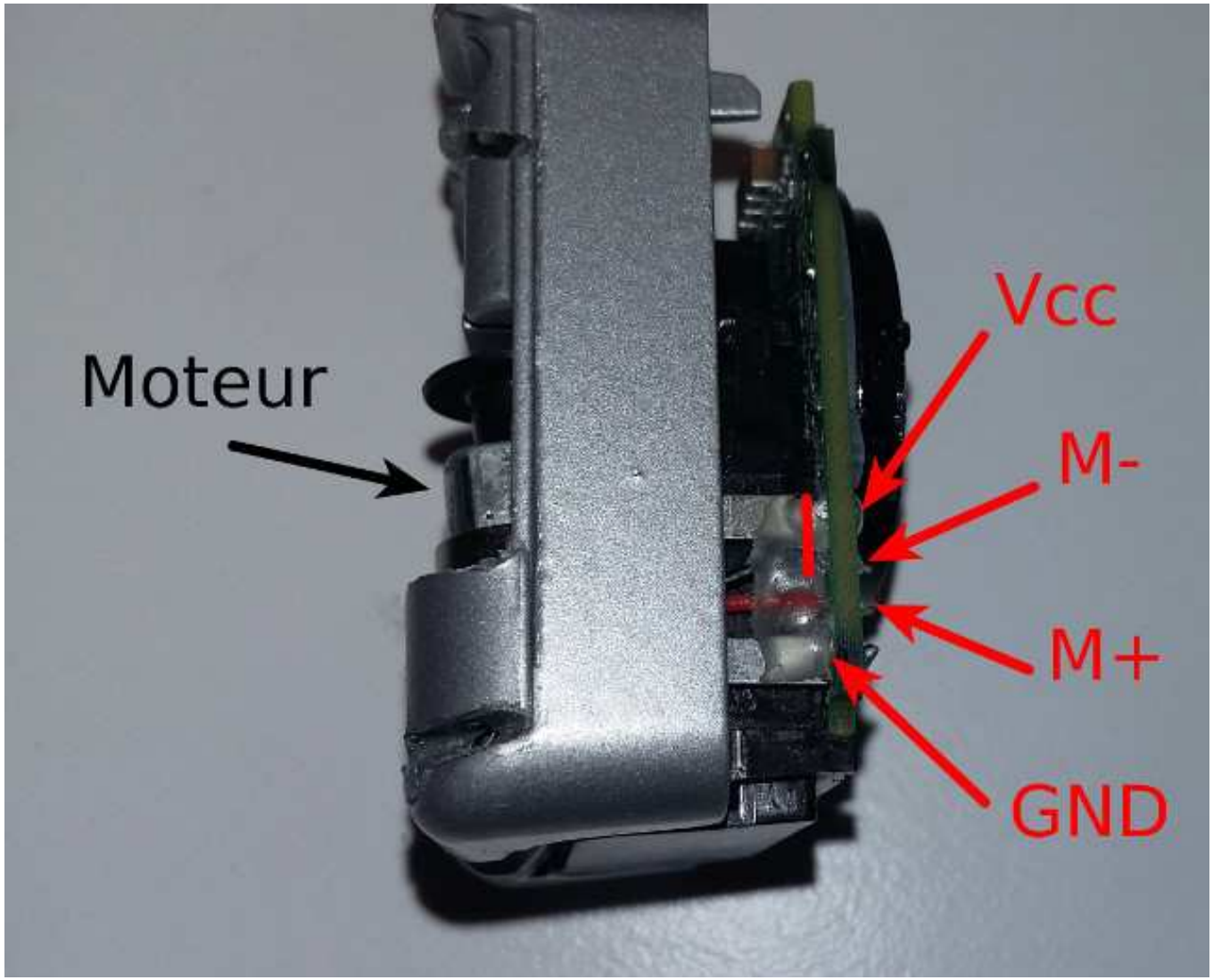


Plusieurs erreurs souvent observées :

- Présence d'indications sur le circuit permettant de localiser les interfaces de débogage ;
- Non-activation des mécanismes de protection de micrologiciel ;
- Erreurs de conception électronique.

Base matérielle

Exemple : erreur de conception électronique



La base logicielle est dépendante de la base matérielle, on distingue notamment :

- Les **micrologiciels monolithiques**, à destination des *uC* et *SoC*
- Les **micrologiciels hétérogènes**, à destination de certains *SoC* et micro-ordinateurs de poche

Base logicielle

Les micrologiciels monolithiques

- Un exécutable unique capable de gérer différentes tâches
- Constitue le système d'exploitation de l'objet
- Dépend de l'architecture du processeur
- Sensible aux vulnérabilités applicatives

Base logicielle
Les micrologiciels hétérogènes

- Un ensemble d'exécutables reposant sur un système d'exploitation
- Généralement stockés en mémoire à l'aide d'un système de fichiers
- Des vulnérabilités peuvent être présentes dans un ou plusieurs des exécutables
- Plus grande surface d'attaque

Base logicielle

Exemple : porte dérobée

- Digital Video Recorder (DVR) connecté en P2P
- Protocole propriétaire, inclut une porte dérobée permettant de lancer une commande en mode administrateur
- Le serveur permet de lister l'ensemble des adresses IP des DVRs connectés
- **Qu'est-ce qui pourrait mal tourner ?**

Base logicielle

Exemple : porte dérobée

Base logicielle

Exemple : porte dérobée

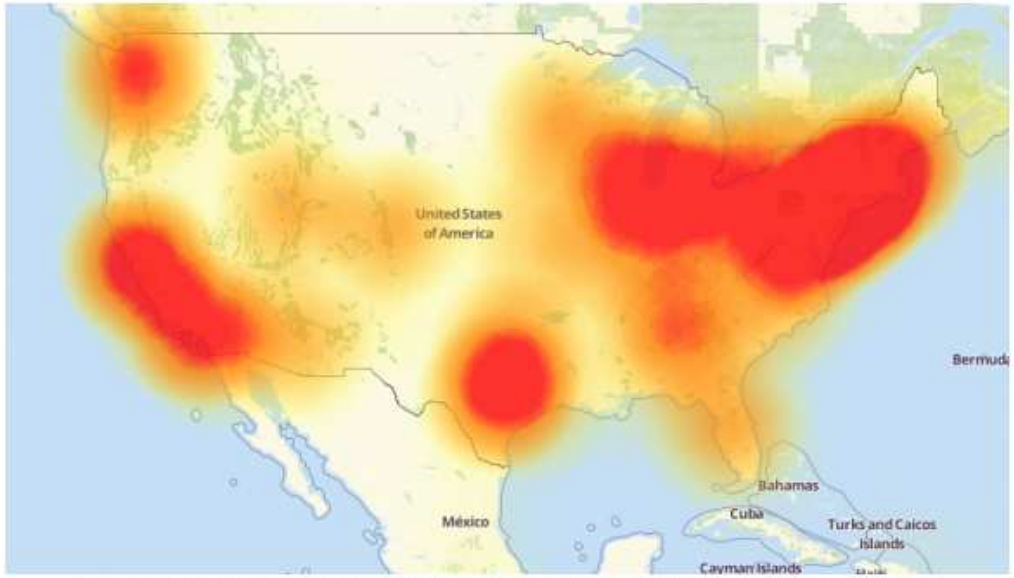
Base logicielle

Exemple : porte dérobée

21 OCT16 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source:

La couche de communication est l'élément liant l'objet au monde extérieur, grâce à des protocoles divers :

- TCP
- UDP
- Bluetooth Low Energy / Bluetooth Smart
- Enhanced ShockBurst (ESB)
- Sigfox
- LoRa / LoRaWAN
- ZigBee
- ...

Couche de communication
Outils d'attaque

La radio logicielle a changé la donne :

- Peu cher (<500$)
- Très pratique car traitement informatique
- Possibilité de réception et d'émission selon les équipements

Couche de communication

Sécurité de la couche communication

Plusieurs erreurs couramment observées :

- **Transmission en clair** de données sensibles
- Absence d'**authentification** des équipements
- Absence de contrôle d'**intégrité**
- **Chiffrement faible** pouvant être cassé

Couche de communication
Exemple de vulnérabilité

Un glucomètre connecté via le protocole Bluetooth Low Energy permet :

- de mesurer le taux de sucre dans le sang
- de conserver un historique des mesures
- d'envoyer les relevés à un ou plusieurs services de télésanté

Couche de communication
Exemple de vulnérabilité

- L'application mobile n'authentifie pas le glucomètre de manière fiable
- Il est possible de se faire passer pour le glucomètre et d'envoyer de fausses mesures (en clair)

Sécurité des objets connectés

Synthèse des erreurs les plus courantes

Cette synthèse est basée sur une vingtaine d'analyses de solutions connectées effectuées au sein du **CERT-UBIK** :

1. Authentification faible ou inexistante
2. Mots de passe par défaut
3. Chiffrement faible ou inexistant
4. Fonctionnalités de débogage activées
5. Absence de fonctionnalité de mise à jour
6. Absence de chiffrement/signature des mises à jour
7. Mauvaise gestion des erreurs
8. Absence de protection physique
9. Absence de fonctionnalité de remise à zéro

(Re)penser la sécurité à l'ère de l'Internet des Objets

(Re)penser la sécurité à l'ère de l'Internet des Objets

La sécurité des systèmes d'information et des objets connectés eux-même doit être adapté afin de prendre en considération :

- Les nouveaux vecteurs d'attaque
- Les **différents environnements** dans lesquels les objets sont placés
- Les **obligations légales** et règlementaires
- Les problématiques liées aux **investigations numériques**

(Re)penser la sécurité à l'ère de l'Internet des Objets

Les nouveaux vecteurs d'attaque

L'intégration de solutions connectées au sein d'un S.I. peut offrir de nouvelles opportunités à un attaquant :

- Les équipements faisant office de **passerelle** permettent le passage d'une technologie à l'autre
- Les **réseaux non-traditionnels** tels que ceux reposant sur la technologie ZigBee peuvent être intrusés sans que cela soit surveillé ni détecté (cf. *Test d'intrusion dans un système de contrôle de la qualité de l'eau*)
- L'utilisation de **réseaux 6LowPAN** permet de rebondir sur des réseaux traditionnels et d'accroître la surface d'attaque

Des outils permettant la surveillance de ces réseaux sont nécessaires

(Re)penser la sécurité à l'ère de l'Internet des Objets

Les différents environnements

Un objet connecté peut être installé :

- Dans les locaux d'une entreprise (accès contrôlé)
- Chez des clients (on parle de *CPE*)
- Dans la nature (sur des rails, des grues, dans la nature, etc.)
- Sur des équipements mobiles (voitures, trains, camions, etc.)
- Sur des êtres vivants (équipements médicaux, animaux, humains)

(Re)penser la sécurité à l'ère de l'Internet des Objets

Equipement installés dans la nature ou mobiles

Ces équipements sont paradoxaux :

- Ils doivent être **peu onéreux** (vol, remplacement)
- Ils doivent tout de même être relativement **bien sécurisés** car ils sont très exposés

Quelques arguments expliquant la faible sécurité de certains objets :

- L'utilisation de chiffrement **réduit significativement** la durée d'utilisation
- L'intégration d'un **Secure Element** a un coût non-négligeable

La compromission d'un équipement ne doit pas aboutir à une compromission massive.

(Re)penser la sécurité à l'ère de l'Internet des Objets

Equipements médicaux (implantés ou extérieurs)

Les équipements médicaux amènent une complexité spécifique :

- Le **remplacement** des équipements implantés **peut être risqué** (défibrillateurs) ;
- L'**intégrité de l'équipement et du porteur** doivent être assurées ;
- Les **données médicales** doivent être protégées.

Les bonnes pratiques de chiffrement, d'anonymisation et d'effacement des données doivent être diffusées et respectées

Les objets connectés médicaux et destinés à la *mesure de soi* facilitent la vie de leurs utilisateurs, mais doivent se conformer à diverses lois et réglementations :

- Loi informatique et liberté
- Code de la santé publique (dossier médical)

(Re)penser la sécurité à l'ère de l'Internet des Objets

Traçabilité et journalisation

La grande majorité des objets connectés ne conservent aucun journal d'évènements :

- l'espace de stockage est très limité (SoC ou uC)
- les concepteurs n'en voient pas l'utilité

Pourtant :

- l'**accès direct** peut être **difficile** sur l'équipement (données volatiles)
- les données non-volatiles sont des **sources importantes d'information** lors d'investigations numériques

Il nous faut des bonnes pratiques en ce qui concerne la journalisation et la traçabilité !

Conclusion

Conclusion

- **Manque d'information** de la part des concepteurs d'objet (technologies utilisées) ;
- La grande majorité des **vulnérabilités touchant les solutions connectées sont classiques et connues**, tout comme leurs contre-mesures (cf. *Entreprise et IoT un mélange instable*) ;
- Ces solutions introduisent de **nouveaux vecteurs d'attaque** à prendre en considération ;
- Les **cadres réglementaires et législatifs** ne sont pas toujours respectés ;
- Pas de prise en compte des **problématiques** liées à l'**investigation numérique** ;
- Des **standards et normes publiées récemment**, mais pas de versions définitives (cf. *State of the art of IETF security related protocols for IoT*)

Questions/Réponses

Contact

digital security | econocom

Site Internet : www.digitalsecurity.fr

Courriel : damien.cauquil@digitalsecurity.fr

Twitter Digital Security : @iotcert

Twitter Personnel : @virtualabs