Comment protéger vos produits et systèmes embarqués

Séminaire Cap'Tronic
9 octobre 2017
Cité internationale universitaire
Paris

Bernard ROUSSELY
bernard.roussely@cyberens.fr

Contenu

- Bonnes pratiques génériques
- Cas des objets connectés
- Conclusions et recommandations

Le problème en catégories

Ludique

Célébrité & notoriété
Ressources limitées
Outils clés en main

Criminel

Vandalisme
Ressources limitées

Hacktiviste

Défend un idéal
Engagé
Bénéficie de réseaux
Attaques ciblées

Crime Organisé

Gain financier
Ressources significatives
Organisation établie
Méthodes transposées au cyberespace

Etatique

Cyberguerre, espionnage
Ressources très importantes
Méthodes sophistiquées

Bonnes pratiques génériques

- Prendre en compte la cybersécurité sur tout le cycle de vie
  - Conception
  - Développement / fabrication (y/c chaîne d'approvisionnement et de distribution)
  - Mise en œuvre (y/c retrait de service)
  - Maintenance
  - Formation des développeurs et des utilisateurs
- Ingénierie de sécurité
  - Analyse de risque
  - Définition d'une architecture de sécurité
  - Fonctions / mécanismes
  - Méthode de validation
  - Gestion des évolutions / mises à jour

Cas des systèmes embarqués

- « Embarqué » peut signifier différentes choses
  - A bord d'un mobile
  - Au sein d'une installation spécifique
  - Objet connecté grand public ou industriel
  - Etc.
- Prendre en compte des contraintes particulières
  - De sûreté de fonctionnement
  - De sécurité
  - De temps de réponse ou de traitement
  - De matériel
  - De consommation d'énergie
  - De forme et d'encombrement
  - Etc.

Focus OC : motivations

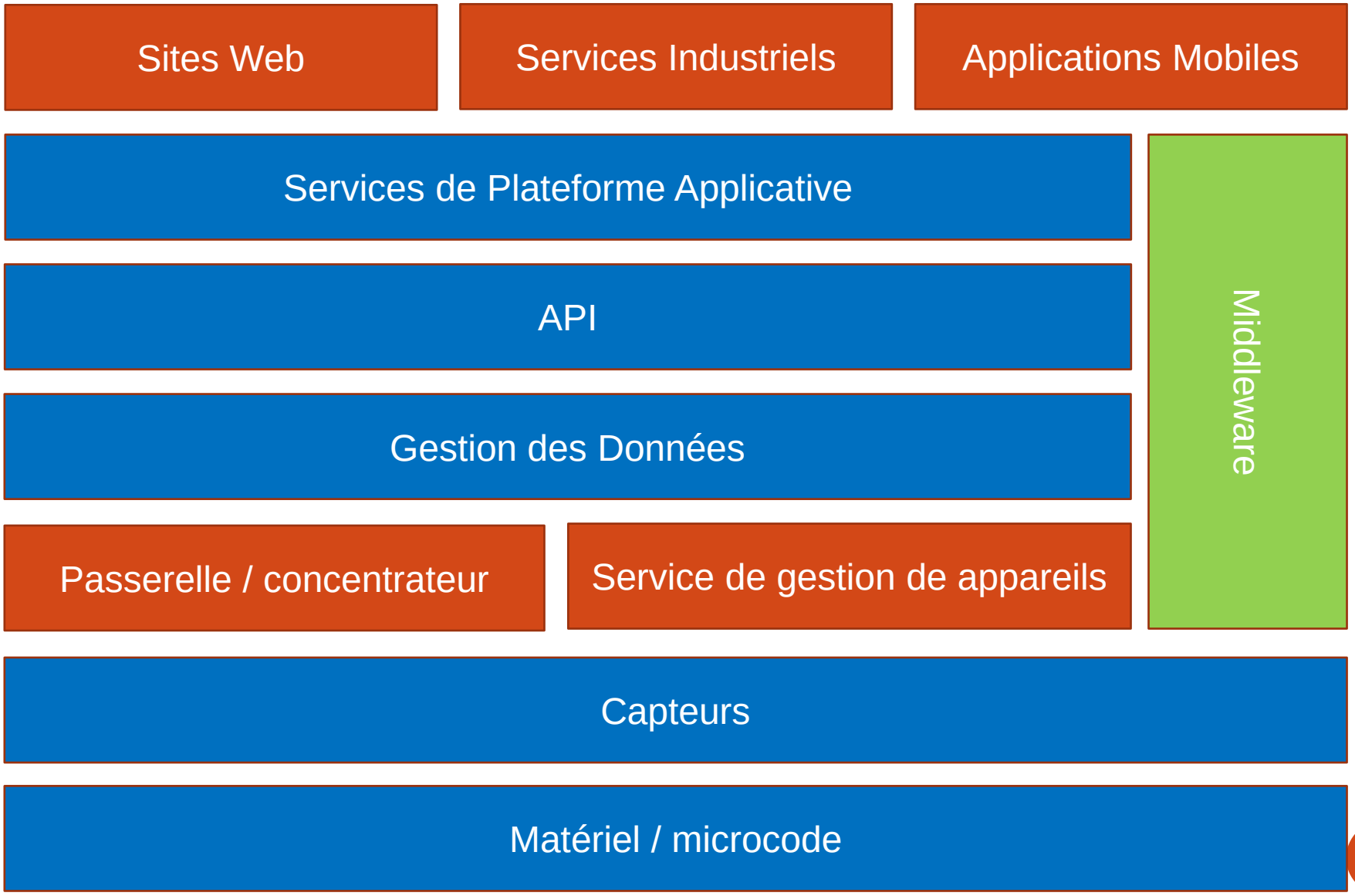
- Au niveau de l'entreprise
  - Réinventer son business model et sa relation client
  - Créer une relation client directe
  - Optimiser ses processus industriels ou non
- Au niveau de l'individu
  - Améliorer le confort personnel (bien-être, santé)
  - Simplifier la vie (domotique, etc.)
  - Apporter de nouveau services

- Une fois les motivations confirmées, garder les RISQUES à l'esprit
  - Les objets connectés augmentent la « surface d'attaque » du SI
  - Atteinte possible à la continuité de service, à l'intégrité et à la confidentialité des données
  - Pour les personnes : atteinte possible à la vie privée

Focus OC : les failles en catégories

- Les **attaques** informatiques exploitent des **vulnérabilités**
  - De conception : spécifications incomplètes, floues ou ambiguës, …
  - De production : erreurs de codage, insuffisance de test, implants, composants non contrôlés
  - De distribution : implant (ajout d'un module non spécifié)
  - Opérationnelles : mauvaise configuration, exploitation défaillante, maintenance non contrôlée, exploitation du retrait de service
  - Humaines : manque de sensibilisation, de formation, de bon sens

Focus OC : architecture logique



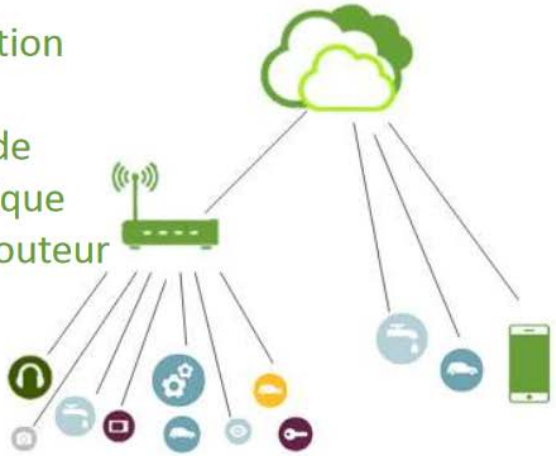
Focus OC : protocoles

- Ces protocoles ne sont pas tous de même nature mais ils ont presque tous la remarquable propriété de ne pas être sécurisés ou d'avoir des failles connues

Focus OC : architectures types

Nécessite un traitement spécifique dans la Gateway (Agent)

Communication directe ou adaptation de liaison physique grâce à un routeur



Focus OC : failles spécifiques (exemples)

- Les **vulnérabilités** principales des objets connectés
  - Absence d'ingénierie de sécurité
    - Pas de coffre fort pour les éléments secrets (clés, MDP)
    - Pas de vérification d'authenticité et d'intégrité des mises à jour
    - Pas de transfert de données protégé
    - « backend » ouvert (serveur dans le « cloud »)
    - Etc.
  - Utilisation de protocoles ayant des failles connues
    - Exemple : BLE < 4.2 (Crackle)
  - Utilisation de protocoles ouverts à tout le monde
    - Exemple : MQTT
  - Utilisation de composants à « bas coût »
    - Performances insuffisantes pour certaines opérations cryptographiques

L’approche et les bonnes pratiques (1/2)

- Conduire une analyse de risque **en amont** sur les OC et leurs interactions
  - Définir le périmètre de l’analyse (cartographie)
  - Identifier les flux et leur sensibilité
  - Identifier les menaces (dont motivations) et les attaques possibles (avec leur impact)
  - Réduire la surface d’attaque, contrôler les chemins d’attaques (contre-mesures)
  - Itérer si conséquence sur architecture ou performances
- Quelques règles simples
  - Former et sensibiliser les développeurs à l’ingénierie de sécurité
  - Rejeter / désactiver d’emblée les protocoles /algorithmes douteux
  - Prévoir le stockage sécurisé des éléments secrets
  - Mettre en place une gestion des correctifs de sécurité et assurer leur diffusion
  - Vérifier l’origine et l’intégrité des MAJ au niveau de chaque sous-ensemble
  - Mettre en place des métriques de sécurité pour suivre les incidents et leurs évolutions (OC, application et « backend »)
  - Se mettre en conformité avec les obligations règlementaires (CNIL, LPM, RGPD, NIS)

L'approche et les bonnes pratiques (2/2)

- Pour un développeur d'objet connecté
  - **Simplifier** les interactions : lutter contre la **complexité**
  - **Réduire** les interactions autant que faire se peut : **automatiser** ce qui peut l'être (et le vérifier)
  - **Contraindre** et **vérifier** toutes les **entrées** faites par un humain (réduire les erreurs intentionnelles ou non) : lutter contre **la loi de Murphy** appliquée à l'utilisateur
  - **Valider** et proposer des **sorties** (actions, affichages, etc.) claires et **non ambiguës**
  - **Vérifier** le système en le **testant** avec exhaustivité (ou en le **prouvant** en partie), en particulier à ses limites
  - Assurer les MAJ et les vérifier avant installation
  - Faire évaluer le résultat par un tiers expert

Conclusion

- La sécurité des objets connectés est un problème très mal traité
  - Prise de conscience difficile des fabricants
  - Connaissances en sécurité des développeurs insuffisantes
  - "Sans budget ni surveillance adéquats, les menaces ne sont pas prises au sérieux et il ne devrait pas être surprenant que les applications mobiles et OC soient responsables des fuites majeures de données à venir", Larry Ponemon, fondateur du Ponemon Institute

- Des solutions simples pourraient améliorer la situation
  - Faire un minimum d'ingénierie de sécurité sur la base d'analyse de risque
  - Appliquer les « bonnes pratiques »
  - Restreindre l'usage en entreprise (réduire la surface d'attaque)
  - Former/sensibiliser les utilisateurs aux risques pour l'entreprise et pour eux-mêmes