

# Sécurité des données des objets connectés

**Journée d'information SRA**  
Vendredi 1<sup>er</sup> décembre 2017

**SRA**  
Sécurité et Réparation Automobiles



**Ronan JEZEQUEL**  
*Ingénieur Développement*  
CNPP

# Sécurité des données des objets connectés

- Introduction : CNPP, Cybersécurité et systèmes connectés
- Vulnérabilités des systèmes connectés
- Solutions pour la prévention et la protection de la cybermenace
- Conclusion



## = > Introduction

- Historique et évolutions du marché
- Etudes CNPP
  - Générale : « cyber »
  - Technique : « objets connectés »

## = > Résultats

- Mise en évidence des faiblesses
  - Produits
  - Installation
- Proposition solutions



## Vulnérabilités des systèmes de sécurité / sureté (1/3)

### = > Approche « matériels »

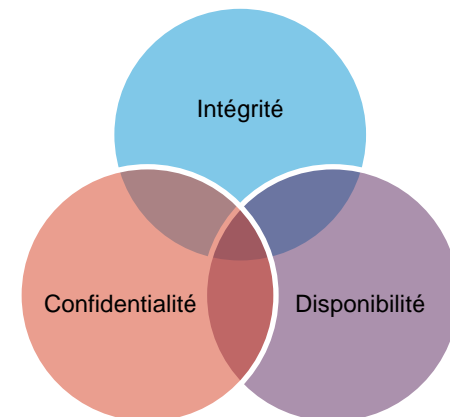


### = > Conséquences des vulnérabilités

#### – Conséquences des vulnérabilités

- Confidentialité ( C )
- Intégrité ( I )
- Disponibilité ( D )

#### – Illustrations : Box sécurité, serrures



## Vulnérabilités des systèmes de sécurité / sureté (2/3)

⇒ Exploitées par des méthodes correspondant à un «état de l'art cybercriminel» de niveau «simple»

### – Exemples de vulnérabilités

- Sur le produit
  - ( C ) Services / ports ouverts par défaut
  - ( I ) Serveur Web sans authentification (http) : Man in the middle
  - ( D ) Champs non assainis dans interface Web
- Au niveau de l'application
  - ( C ) ID / MdP fabricant par défaut
  - ( I ) Téléchargement des MàJ non sécurisé
  - ( D ) Manipulation provoquant arrêt
- Protocoles
  - ( C ) Sniffing : données en clair
  - ( I ) Rejeu OK
  - ( D ) Absence de réaction au brouillage



## Vulnérabilités des systèmes de sécurité / sureté (3/3)

### = > Approche « Système »

#### – Vulnérabilités liées à l'installation ⇔ vulnérabilités du SI

- Mauvaise architecture / Cloisonnement
- Insuffisance voire absence de protection des données (chiffrement, etc..)
- Défaut de sensibilisation personnel + mauvaise « hygiène » SI
- Absence de mise à jour et de suivi régulier

#### – Recommandations pour l'installation

- Analyse risque numérique
- Formulation d'exigences
  - Conception
  - Réalisation
  - Exploitation / Maintenance
- Prise en compte dans certifications services



## Solutions pour la prévention et la protection de la cybermenace (1/2)

- **Produits développés pour la réalisation et la maintenance de l'installation**
  - Référentiel APSAD D32
  - Formation
- **Produit développé pour l'évaluation de la robustesse des produits (ST SOC – DEC 17 05)**
  - Applicable à tout type de produit connecté
  - Déclinée en fonction de la « composition » du produit
  - Méthode
    - Relevé des vulnérabilités
    - Exploitation
    - Evaluation de la criticité des vulnérabilités
  - Livrable brut : Rapport d'analyse de la robustesse aux attaques numériques



## Solutions pour la prévention et la protection de la cybermenace (2/2)

### – Application « simple » de la ST SHOC

- Délivrance d'un rapport listant les vulnérabilités
- Objectif : Aide au développement ou préparation de la certification



### – Application via les référentiels de certification produits

- Evolution : Cumul évaluation « classique » et évaluation cyber
- Complément cyber = exigences relatives au résultat de l'analyse « ST SHOC » (ex : x boucliers)
- Avec délivrance d'un certificat « CNPP certified », « A2P@ », « NF&A2P@ ».. Attestant de la **double performance** « **sécurité physique / sécurité logique** »
- Exemples : EVN (arrêté 03/08/2007 modifié), Serrures connectées, d'alarmes etc..



### – Autres essais cyber

- Selon exigences spécifiques normalisées (ex : EN 1300 – serrures coffre fort)
- Vérifications selon document tiers (ex : guide ANSSI – systèmes contrôle d'accès)



## Conclusion

- **Déploiement de solutions**
  - Techniques
  - Organisationnelles
- **Méthode d'évaluation « ST SOC » applicable à tout produit commercialisé sous la forme « connectée »**
- **Traduction des résultats obtenus en exigences pour l'évaluation de la conformité selon référentiels existants :**
  - Référentiels de certification
  - Documents tiers (ex : guide ANSSI)
- **Opportunité de mise à jour des cahiers des charges SRA**



**Merci de votre attention!!**

**Contact :**

**Ronan JEZEQUEL**

**02 32 53 99 38**

**[ronan.jezequel@cnpp.com](mailto:ronan.jezequel@cnpp.com)**