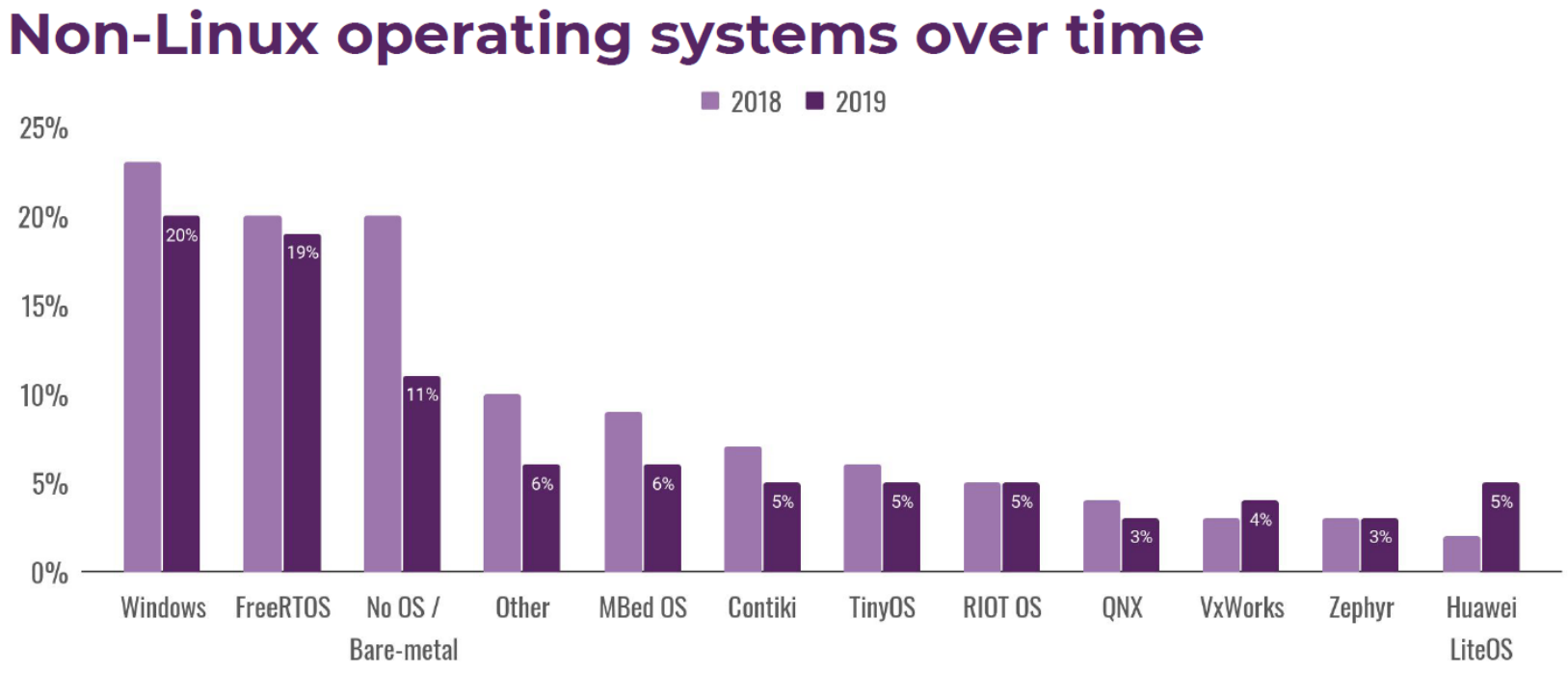
OS POUR SYSTÈMES EMBARQUÉS

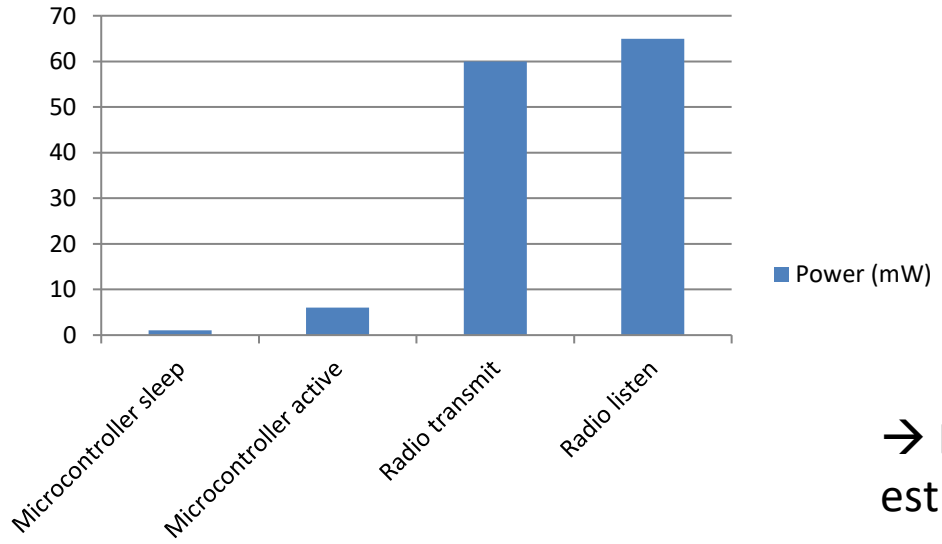
OS pour IoT



Source: IoT Developer Survey 2019 Results from eclipse.org

Management de l'énergie

- L'énergie pour IoT est une ressource limitée, de fait l'économie d'énergie doit se faire aussi bien au niveau matériel que logiciel.
- Pour les objets intelligents équipés de radio, l'émetteur-récepteur est le composant le plus énergivore (près de dix fois que le microcontrôleur en mode actif).



→ Le processus d'écoute active est très couteux en énergie consommée

SÉCURITÉ EMBARQUÉE

Introduction – part I

- Qu'est-ce que la **sécurité** ? C'est protéger le système contre un adversaire déterminé.

- Les objets intelligents ne sont pas à l'abri d'attaques ou de vols de données. Il est important d'intégrer de la sécurité.

- Les objets intelligents ont des ressources limitées, ces contraintes influencent l'implémentation de leur sécurité.

Introduction- part - II

- **L'intégrité :** garantir que les données sont authentiques
- **La disponibilité :** maintenir le bon fonctionnement du système d'information
- **La confidentialité :** rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction
- **La non-répudiation** : garantir qu'une transaction ne peut être niée
- **L'authentification :** assurer que seules les personnes autorisées aient accès aux ressources

Introduction- part - II

- **L'intégrité :**

  Il faut garantir et préserver la validité et l'exactitude des données durant tout son cycle de vie. On distingue généralement deux types d'intégrité dont les processus et méthodes peuvent varier :

  - **Intégrité physique** : protection de données uniques et exactes lorsqu'elles sont stockées et récupérées.

  - **Intégrité logique** : conservation inchangée des données au cours de leurs manipulations multiples (au niveau d'une base de données relationnelle, par exemple).

- Solution : Message Integrity Code

Introduction- part - II

- **La disponibilité :**

  Les doivent être accessible et disponible en permanence pour toutes les personnes autorisées.

  Cela permet de ne pas être pénalisé en passant à côté d'informations cruciales pour une prise de décision ou bien ne pas pouvoir accomplir une tâche ou une fonction.

  Cet aspect de la cybersécurité est difficile à garantir dans l'IoT , particulièrement dans les systèmes de communication sans-fils.

Introduction- part - II

- **La confidentialité :**

  L'objectif de la confidentialité des données est de maintenir une non-divulgation des données et/ou leur non-accessibilité aux personnes ou systèmes informatiques non autorisés.

Introduction- part - II

- **La non répudiation :**

  La non-répudiation des informations a pour but d'assurer que l'émetteur d'une information ne soit pas en mesure de nier qu'il est bien à l'origine de celle-ci.

  Pour atteindre cet objectif de la sécurité informatique on utilise, par exemple, la signature des emails, des documents ou des certificats.

  Ainsi, seul l'utilisateur possédant une clé privée peut apposer sa signature sur un email et cette personne ne pourra pas nier en être l'émetteur.

Introduction- part - II

- **L'authentification :**

  L'authentification permet d'assurer l'identité d'un utilisateur grâce à l'usage d'un code d'accès : ici, l'objectif de la sécurité informatique est de garantir que chaque utilisateur est bien celui qu'il dit être.

  Le contrôle d'accès, par un mot de passe par exemple, permet de limiter la consultation ou l'utilisation de certaines ressources seulement aux personnes autorisées.

  A noter qu'il ne faut pas confondre identification et authentification.

  L'identification est une phase qui consiste à établir l'identité de l'utilisateur (qui je suis).

  L'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité (par un code secret ou avec « Message Authentification Code»)