# Développement d'un pare-feu domestique

## Présentation du projet (MAB1 Info)

Rémy Decocq

Faculté des Sciences
Université de Mons


05/09/19

# Outline

# Organisation du projet

## $1^{ere}$ partie

État de l'art

- aspect "domestique"
  $\rightarrow$ *IoT, smarthome*
- motivations pour la protection de tels réseaux
- aspect "sécurité"
  $\rightarrow$ *pare-feux, IDS, scanneurs*

## $2^{eme}$ partie

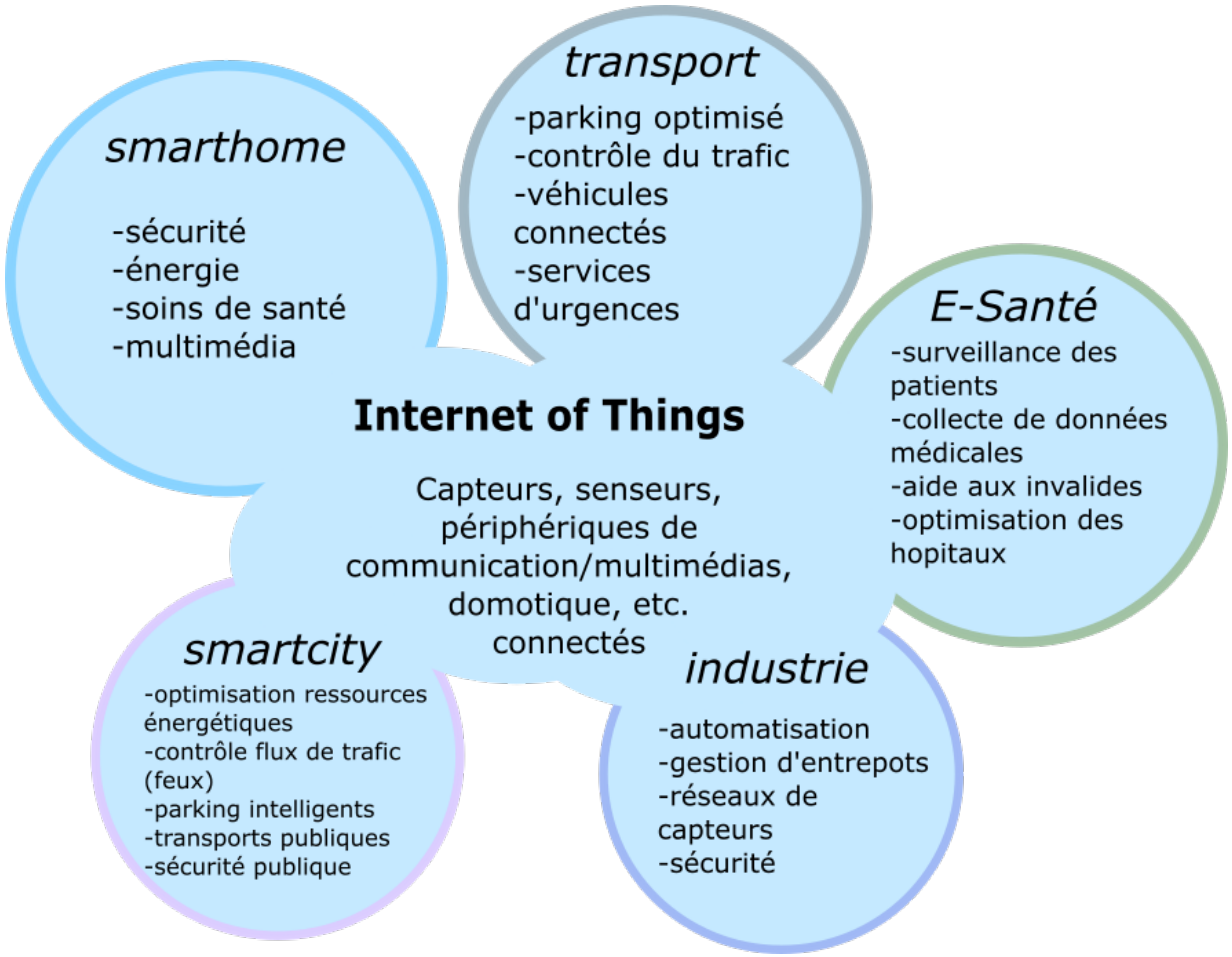
Développement d'une application

- contexte et motivations
- présentation des concepts
- déploiement et tests

# Outline

# L'Internet des Objets (IoT)

Pas de définition acceptée à l'unanimité



# Les restrictions des équipements IoT

- contraints en ressources CPU, mémoire et radio
- requièrent une faible consommation énergétique
- programmés à un bas niveau d'abstraction
- conçus pour satisfaire une unique fonction

---

Relègue la sécurité au second plan

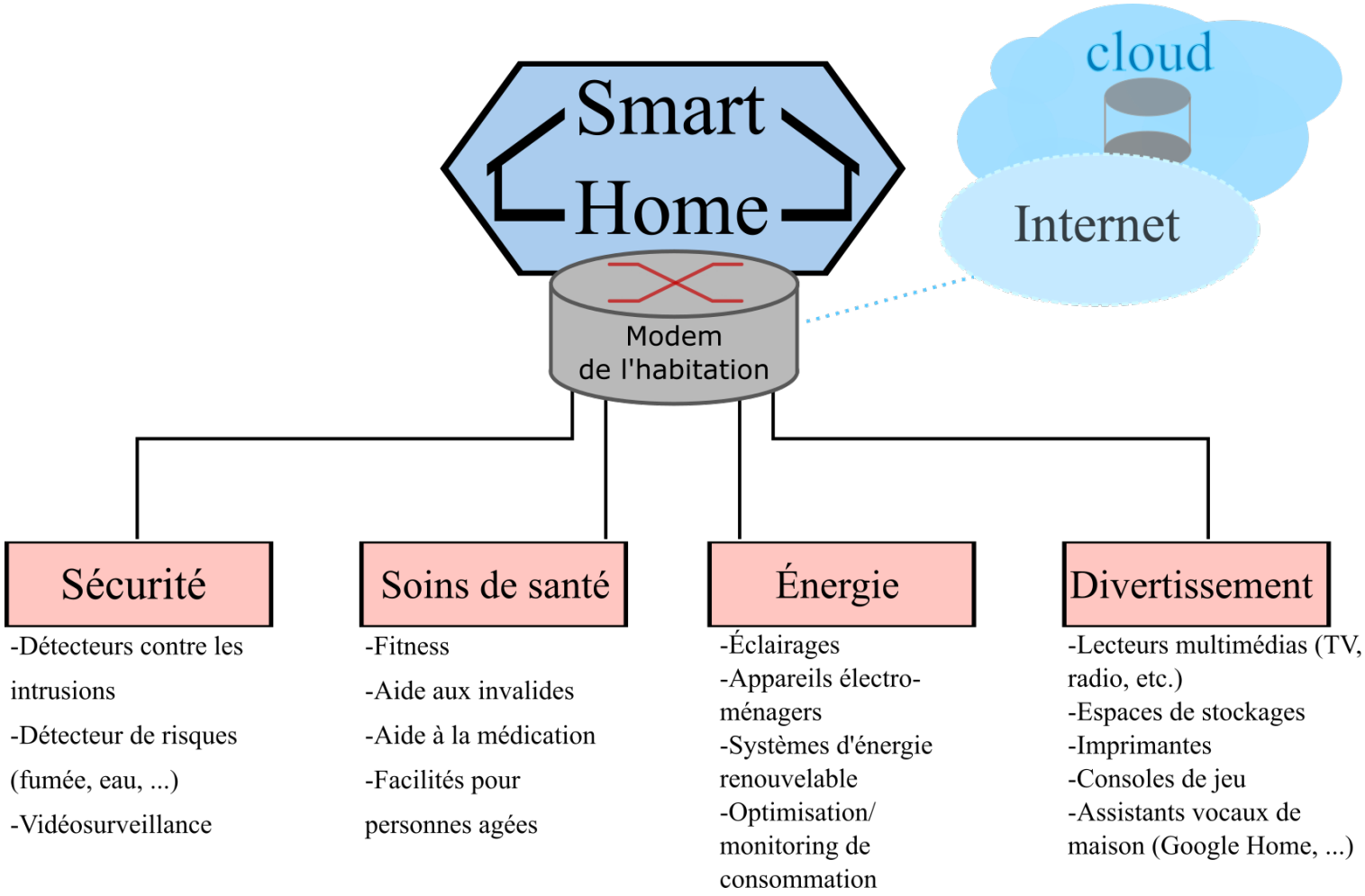
# Protocoles adaptés aux équipements restreints

Les restrictions ont mené à l'élaboration de nouveaux standards et protocoles

| Couches du modèle | *Protocoles de la stack IoT* | *Protocoles de la stack TCP/IP* |
|---|---|---|
| **Application** | IETF CoAP \| MQTT \| ... | HTTP \| FTP \| DNS \| ... |
| **Sécurité** | DTLS | TLS |
| **Transport** | UDP | TCP \| UDP |
| **Réseau** | IPv6 \| IETF RPL | IPv4 \| IPv6 |
| **Adaptation** | IETF 6LoWPAN | Non défini |
| **Lien** | IEEE 802.15.4 MAC | Dépend du média et de la technologie (IEEE 802.11 WiFi, Ethernet, ...) |
| **Physique** | IEEE 802.15.4 PHY | |

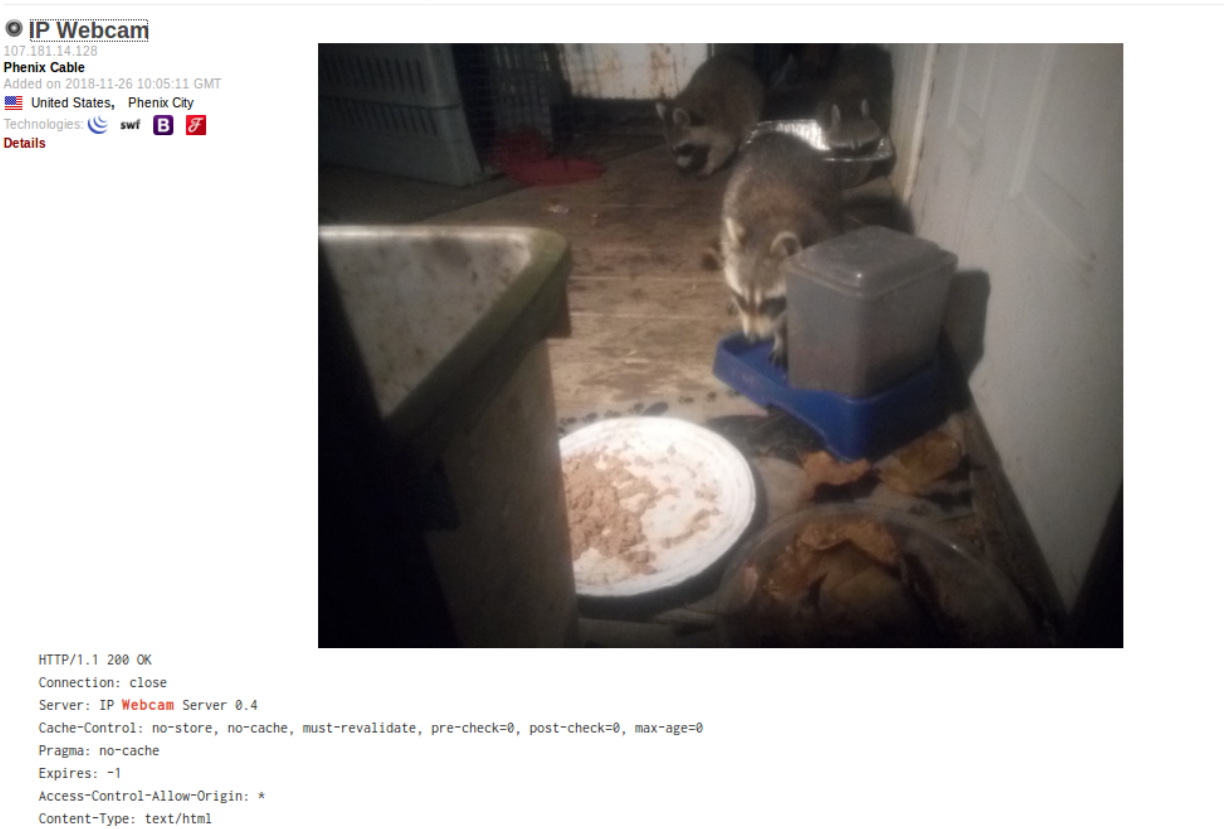
# L'environnement *smarthome*

On compte en moyenne 11 *smart devices* par habitation (USA)



# Pourquoi la sécurité dans l'IoT ?

- Équipements vulnérables utilisés par des botnets (*Mirai*, *Reaper*, ...) dans des attaques de masse
- Atteinte à la vie privée facilitée (démo avec l'outil *Shodan*)



# Protéger les smarthomes : les pare-feux

- Pare-feux niveau hôtes → non ou peu compatible avec les restrictions de l'IoT
- Pare-feux niveau réseau :
  - filtrage effectué en bordure du réseau domestique
  - sur une machine non restreinte (modem/routeur)
  - utilisant des techniques plus ou moins avancée

  sous différentes formes : software sur le modem ou machine dédiée :


FIGURE – Cisco ASA 5506H - Appliance dédiée

FIGURE – b-box 3 - modem domestique

# Protéger les smarthomes : les NIDS

Pare-feux → filtrent les paquets, bloquent selon des règles

NIDS, *Network Intrusion Detection System* :

- capturent et analysent le trafic et les évènements dans le réseau à protéger mais n'**intervient pas de façon directe**
- lancent des alertes à destination de l'utilisateur/administrateur suite à la détection de menaces

L'analyse du trafic se repose sur 2 techniques de détection :

1. par signature : bdd de signatures d'attaques connues + *pattern matching*
2. par anomalies : heuristiques combinées à des profils types

# Protéger les smarthomes : les scanneurs

# Outline

# Idée générale

# Concepts

# Déploiement

# Tests sur un réseau virtuel

# Tests dans un environnement réel

# Conclusion

# Développement d'un pare-feu domestique

# FAQ