Plateforme d'expérimentation pour la sécurité des objets connectés

Florent Galtier, Paul Olivier, Vincent Nicomette, Guillaume Auriol,
Philippe Limousin, Radhouene Azzabi
LAAS-CNRS, CEA-tech Occitanie
- 12/07/2024 -

Plan de la présentation

- PEPR SuperviZ
- Objectifs
- Expérimentations
- Perspectives

PEPR Cybersécurité - SuperviZ

Supervision de la sécurité

1. Identifier et gérer le risque
2. Détecter les attaques
3. Résister et répondre aux attaques
4. Rendre la supervision sûre
5. Concevoir des méthodes de validation des méthodes de détection
6. Développer des plateformes d'expérimentation

FRANCE 2030

Problématique

Protocoles sans-fil de l'IoT :

- Nombreux
- Souvent en source fermée

Objets connectés :

- Peu sécurisés
- Hétérogènes

> **Expérimentations en sécurité nécessaire, mais difficiles à mettre en place/reproduire**

Objectif de la plateforme

- **Génération de datasets de trafic légitime ou d'attaque**
  - Capture de trafic à l'aide de sondes (USRP B200 mini)
  - Analyse via logiciel défini par l'utilisateur, ou via détection de modulation simple
- **Test de méthodes de détection d'intrusion**
  - Possibilité d'embarquer un IDS sur une machine locale disposant de sondes

Expérimentations possibles

> Génération du trafic légitime

- Présence de divers objets IoT grand-public de différents types (thermomètre, caméra, prises…) utilisant différents protocoles (BLE, Zigbee, WiFi…), contrôlables à distance

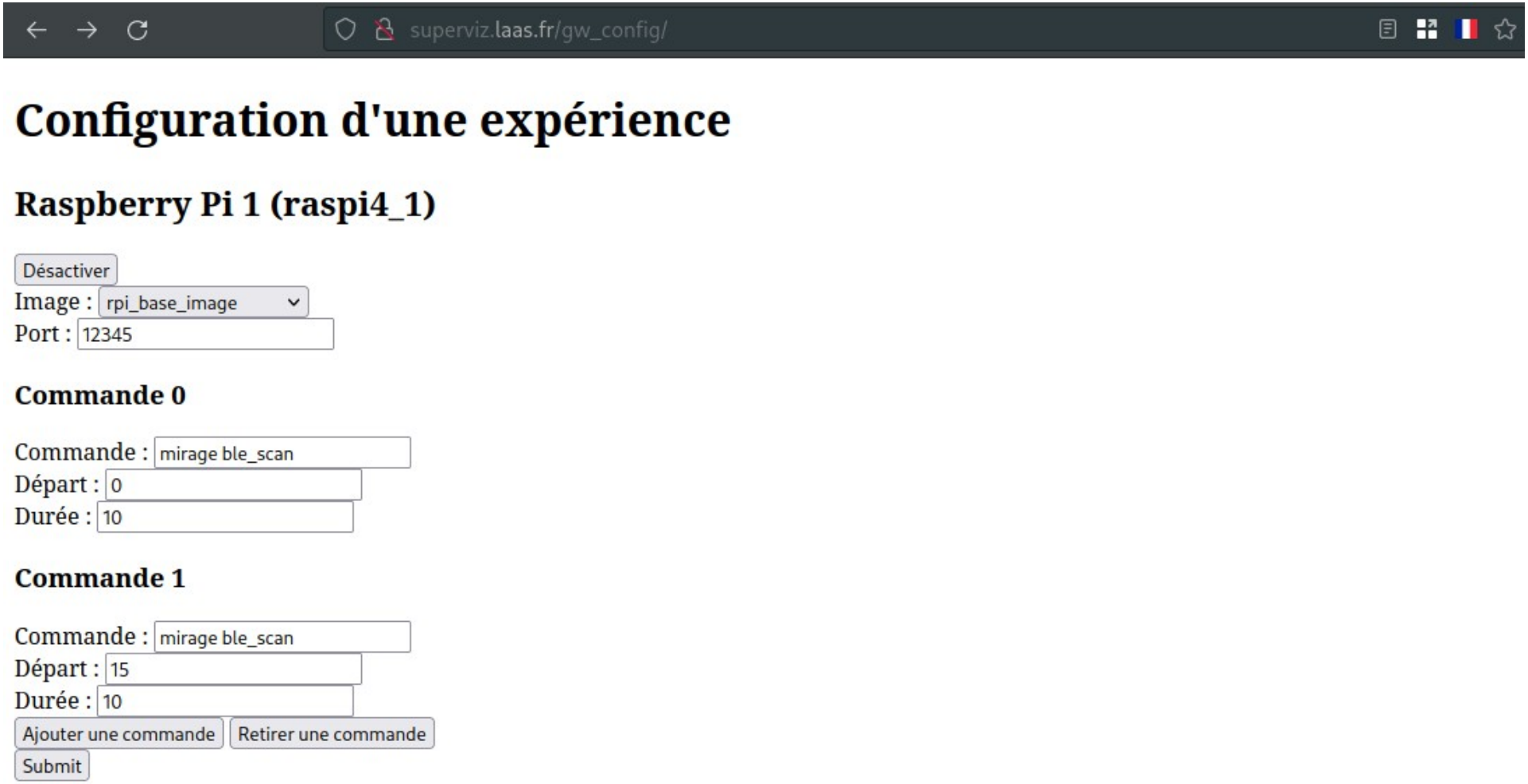
> Génération du trafic d'attaque

- Implémentation d'attaques de l'état de l'art sur des Raspberry Pi

> Contrôle complet de l'environnement

- Isolation à l'aide d'une cage de Faraday
- Contrôle à distance des objets émettant ou non dans l'environnement

Interface de configuration



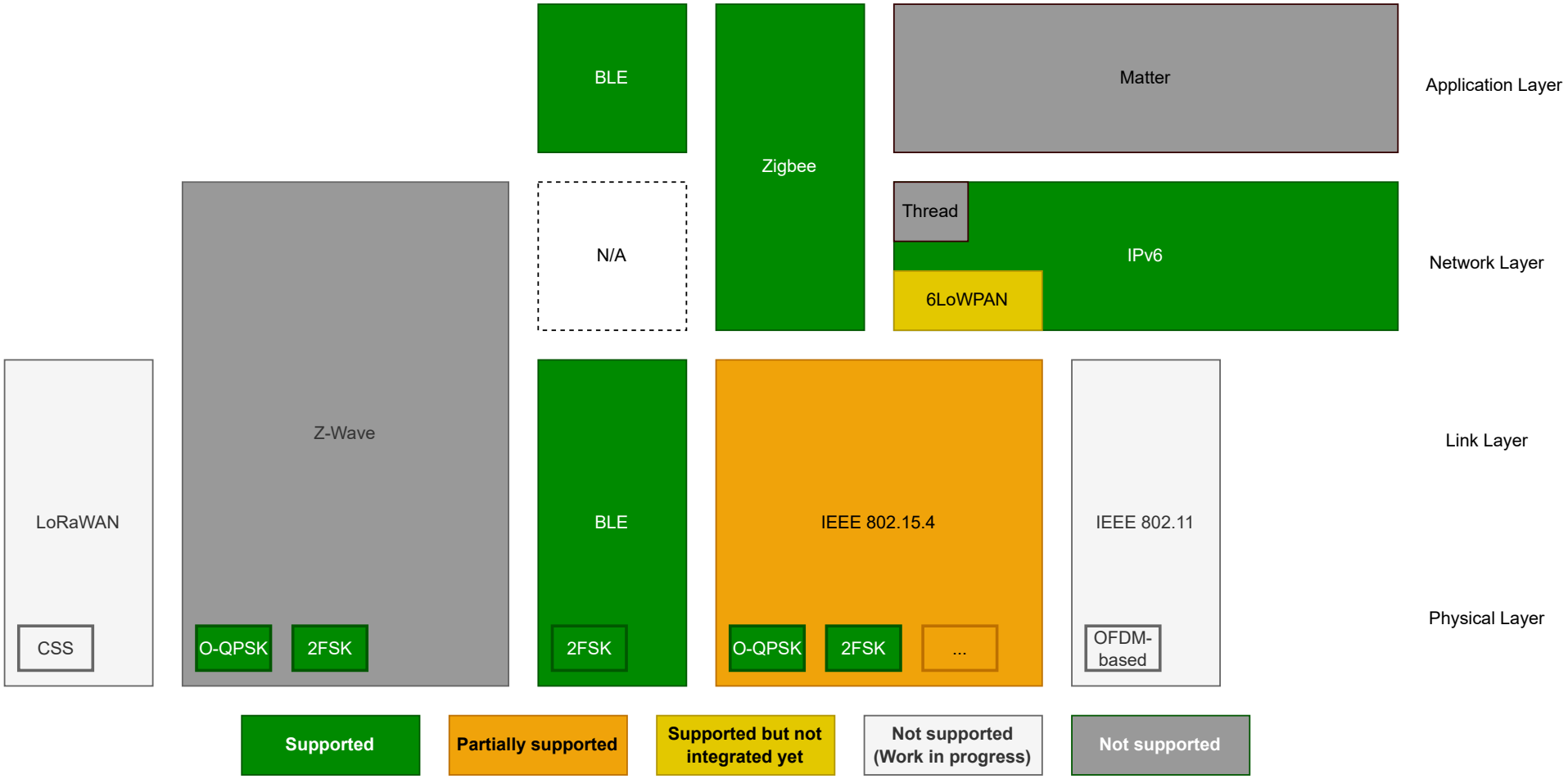
Configuration directe

```
{
        "devices": [
                {"type": "raspi", "image": "rpi_base_image_bak", "addr": "192.168.1.1", "port": "12345", "cmds": [
                        {"mirage": "mirage ble_scan", "time": "0", "duration": "10"}
                ]},
                {"type": "other", "name": "BEEWi Smart Plug", "status": "1"},
                {"type": "other", "name": "BEEWi Smart Power Plug", "status": "1"},
                {"type": "other", "name": "Philips Hue Bridge", "status": "1"},
                {"type": "other", "name": "Tado Smart Thermostat", "status": "0"}
        ],
        "radios": [{"fc": "2402e6", "fs": "4e6"}]
}
```

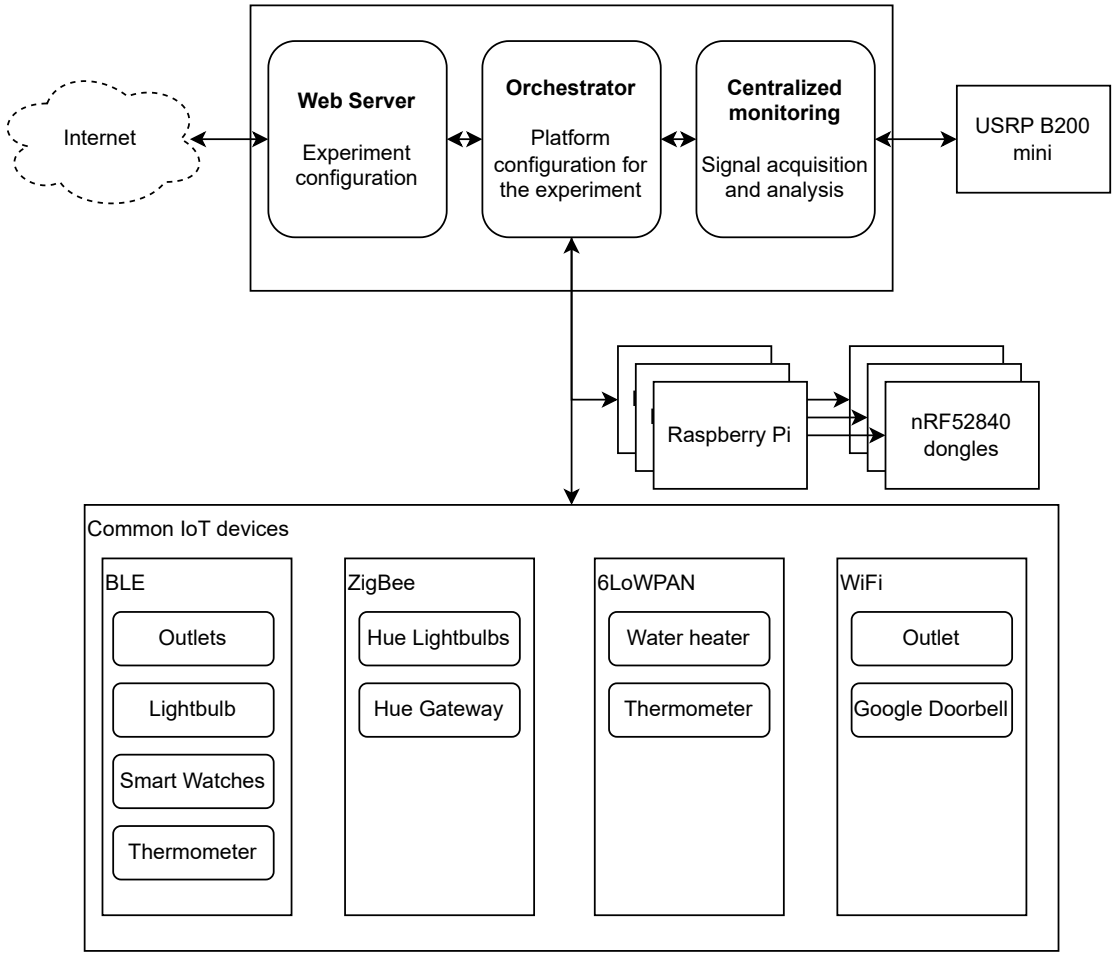
Collecte des résultats

- **Remontée des logs des attaques**
  - Utilisation du framework Mirage
- **Remontée des logs des IDS**
- **Remontée des captures brutes des sondes**
  - Possibilité d'ajout de logiciels d'analyse pour remonter d'autres formats, type pcap

Protocoles supportés



Matériel actuel



Merci pour votre attention

Ce travail a bénéficié d'une aide de l'état gérée par l'Agence Nationale de la Recherche au titre de France 2030 portant la référence ANR-22-PECY-0008. Les opinions exprimées dans ce document ne reflètent pas nécessairement l'avis du gouvernement français.