

# Cahier des charges : Wireless Attack Network Testbed for Embedded Devices

## 1 Contexte et justification

La plateforme WANTED est un testbed pédagogique/expérimental pour évaluer la sécurité des dispositifs IoT embarqués. L'extension proposée vise à intégrer, implémenter et orchestrer des attaques LoRa / LoRaWAN afin d'évaluer les résistances des réseaux et des devices dans un environnement contrôlé. L'objectif est de fournir des scénarios reproductibles, des plugins d'attaque intégrés à WANTED et des playbooks de test pour la recherche et la formation.

## 2 Objectifs

### 2.1 Objectif général

Fournir, pour LoRa/LoRaWAN, une suite d'attaques intégrées et testées dans la plateforme WANTED permettant d'évaluer la robustesse d'un réseau et d'appareils IoT.

### 2.2 Objectifs spécifiques (à la fin du premier mois)

- Intégrer les attaques existantes dans WANTED
- Implémenter des nouvelles attaques pour LoRaWAN
- Produire des scénarios de test automatisés et scripts de reproduction
- Rédiger la documentation d'intégration (README)

## 3 Périmètre (ce qui est inclus / exclu)

### 3.1 Inclus

- Attaques actives et passives ciblant LoRa/LoRaWAN en laboratoire contrôlé
- Intégration en tant que plugins/modules dans l'architecture WANTED (interfaces start/stop/status)
- Tests sur un réseau de test isolé (gateways, Network Server local ex. ChirpStack, end-devices programmables)
- Documentation et scripts d'automatisation

### 3.2 Exclu

- Tests sur réseaux publics/production ou appareils appartenant à des tiers sans autorisation écrite
- Attaques visant à extraire des clés cryptographiques réelles sur matériel tiers sans consentement
- Déploiements commerciaux/industrialisation du module (prototype/POC uniquement)

## 4 Contraintes Techniques

- **Délais** : Projet à réaliser sur 3 mois séparés (cycle : 1 mois actif, 1 mois pause, 1 mois actif...), démarrage : premier mois actif
- **Normes** : Respect des normes de sécurité et de communication.

## 5 Livrables

- Code source des plugins/attaques (répertoire `wanted/attacks/...`)
- Scripts d'automatisation et tests (pytest / scripts bash)
- Environnement de test documenté (chessboard : VM, ChirpStack, gateway config)
- Documentation détaillée : README.
- Rapport final synthétique et recommandations (contre-mesures)

## 6 Exigences fonctionnelles (F)

- F1. Chaque attaque doit exposer une interface commune : `start(params)`, `stop(id)`, `status(id)`
- F2. Les attaques doivent produire des logs JSON structurés (timestamp, niveau, message, métriques)
- F3. Possibilité de configurer paramètres : fréquence, durée, payload, répétitions
- F4. Intégration avec WANTED via REST/CLI (authentification interne de la plateforme)
- F5. Tests automatisés pour chaque attaque (scénarios de réussite/échec mesurables)

## 7 Exigences non-fonctionnelles (NF)

- NF1. Isolation réseau : toutes les expérimentations doivent se dérouler dans un réseau de labo isolé (VM, VLAN)
- NF2. Traçabilité : journalisation complète des opérations et des paramètres de tests
- NF3. Reproductibilité : scripts et instructions claires pour reproduire chaque scénario
- NF4. Sécurité : mécanismes pour arrêter immédiatement toute attaque (kill switch)