

# Audit de Sécurité : Coffre-fort RF

## Reverse Engineering de protocoles radio et injection de trames

### Résumé exécutif

Audit de sécurité d'un coffre-fort 433 MHz. J'ai réalisé le reverse engineering du protocole propriétaire et développé un système d'injection automatisé pour démontrer les vulnérabilités du verrouillage.

### Défi

Identifier une trame radio inconnue en environnement bruité. L'enjeu était de concevoir un algorithme capable de décoder les bits variables en temps réel pour une attaque par force brute.

### Ce que j'ai construit

**Architecture** : Antenne RF → Récepteur SDR (USRP) → GNU Radio → Script Python.

**Composants clés** : USRP, GNU Radio, Blocs Python (Seuil dynamique), Interface PyQt5.

## Compétences démontrées

- Radio Logicielle (SDR) et analyse de protocoles
- Développement Python et traitement du signal
- Cybersécurité et audit de vulnérabilité
- Reverse Engineering RF

## Résultats & Impacts

- **Succès** : Décodage total de la trame de 38 bits (PROEM).
- **Fiabilité** : 100% de lecture via seuil dynamique auto-adaptatif.
- **Vitesse** : Injection à 2000 bits/s pour un craquage optimisé.

## Équipe et rôle

---

Réalisé en binôme. **Mes contributions clés** : Création de la chaîne de réception sur GNU Radio, développement du script de décodage et de l'interface de monitoring.

---

**Projet** : Électronique & SDR | **Livrables** : Script d'attaque, Rapport d'audit | **Tech** : Python, GNU Radio  
Portfolio Arthur Blanc - arc421.fr