PROJET: WIRELESS ATTACK NETWORK TESTBED FOR EMBEDDED DEVICES (WANTED)

Réalisé par: Meysoun Gharbi
Encadré par: Philippe Tanguy

PLAN

1- Contexte

2- Modèle de menace

3- Cahier de charges fontionnel et technique

4- Retroplanning

CONTEXTE

LoRaWAN, le protocole pour les réseaux étendus à basse consommation (LPWAN) basés sur LoRa, n'a pas été conçu délibérément avec une « mauvaise sécurité ». Il intègre en réalité des mécanismes de sécurité pour protéger les données et les communications entre les appareils et le réseau. Comme toute technologie, il présente néanmoins des vulnérabilités et des défis, générant des risques potentiels.

Pour répondre à ces problématiques et renforcer la sécurité de LoRaWAN, je contribue au projet WANTED. Il s'agit d'une plateforme d'orchestration d'expérimentations de sécurité qui permet d'exécuter, de tracer et d'analyser des attaques en laboratoire isolé. Son objectif est d'identifier des vulnérabilités et de proposer des contre-mesures.

MODÈLE DE MENACE

Le modèle de menace est une représentation structurée de toutes les informations pour la sécurité du système. En clair, c'est le processus qui consiste à se poser les bonnes questions pour identifier:

- Ce que je veux protéger (les actifs)?
- Contre qui/quoi je veux le protéger (les objectifs et les motivations d'un attaquant)
- Comment l'attaquant pourrait s'y prendre (les vecteurs d'attaque)
- Quelles seraient les conséquences s'il réussirait
- Comment je vais me défendre (les contre-mesures).

Qu’est ce que je veux protéger ?: (les actifs)

Actif	Confidentialité	Intégrité	Disponibilité	Impact Global
1. Données Temps Réel	MODÉRÉ Renseignement industriel	CRITIQUE Décisions erronées + risques sécurité	CRITIQUE Aveuglement opérationnel	MAXIMAL
2. Serveurs Centraux	ÉLEVÉ Vol de données + secrets	CRITIQUE Compromission persistante	ÉLEVÉ Arrêt système	MAXIMAL
3. Passerelles (Gateways)	MODÉRÉ-ÉLEVÉ Écoute communications	CRITIQUE Injection données + relais attaques	ÉLEVÉ Point de défaillance unique	MAXIMAL
4. Network Server	ÉLEVÉ Accès total réseau	CRITIQUE Contrôle entier du réseau LoRaWAN	CRITIQUE Arrêt réseau complet	MAXIMAL
5. Capteurs IoT	FAIBLE-MODÉRÉ Données individuelles	ÉLEVÉ Source données corrompues	ÉLEVÉ Perte couverture zone	ÉLEVÉ
6. Processus JOIN	CRITIQUE Vol clés sécurité	CRITIQUE Intrusion devices malveillants	MODÉRÉ Blocage nouveaux devices	MAXIMAL

Qu’est ce que je veux protéger ?: (les actifs)

Niveau 1: Critique Maximal

1- Network server: Coeur du système
2- Processus Join: Porte d’entrée réseau
3-Intégrité données: Temps-réel et sécurité opérationelle

Niveau 2: Haute priorité

4- Passerelles: Point de transit critique
5- Serveurs centraux: Infrastructure du backend

Niveau 3: Priorité moyenne

6- Capteurs individuels: Impact localisé

Contre qui/quoi je veux le protéger ?: (les objectifs et les motivations)

De qui?

- Acteur malveillant générique (hacker opportuniste, script kiddie)
- Concurrent malveillant (entreprise concurrente, espion industriel)
- Activiste/terroriste (groupe organisé, motivations idéologiques)

Motivations/objectifs

- Motivations financières (vols de données pour revente sur darknet/ manipulation des données métier/ sabotage de concurrents)
- Motivations stratégiques (vol de secrets de fabrication/ accès aux données stratégiques/ Déstabilisation concurrents perturbation marché)
- Motivations idéologiques (protestation contre une organisation/ Perturbation d'infrastructures critiques/ message politique ou social)
- Motivations personnelles (prestige dans la communauté hacker/ curiosité technique ou défi intellectuel/ vengeance: ancien employé mécontent)

Comment l’attaquant peut s’y prendre ? (vecteurs d’attaque)

1- Attaque de manipulation d’ADR

- **Cible** : Network Server + Capteurs
- **Mécanisme** : Envoi de commandes ADR malicieuses
- **Résultat** : Augmentation collisions + perte de couverture

2-Attaque de synchronisation de Beacon

- **Cible** : Synchronisation réseau entier
- **Mécanisme** : Injection de beacons temporels falsifiés
- **Résultat** : Communications coordonnées impossibles

3- Attaque de Frame Counter

- **Cible :** Intégrité des communications
- **Mécanisme :** Exploitation faiblesses gestion compteurs de trame
- **Résultat :** Contournement protection anti-replay

4- Injection d’une commande Mac

- **Cible :** Contrôle MAC layer
- **Mécanisme :** Injection commandes MAC malicieuses
- **Résultat :** Reconfiguration malveillante capteurs

5- Attaque SF targeting

- **Cible :** Performance réseau
- **Mécanisme :** Brouillage sélectif par Spreading Factor
- **Résultat :** Attaque discriminatoire types capteurs

6- Exploitation de duty cycle

- **Cible :** Conformité réglementaire
- **Mécanisme :** Forçage violation duty cycle
- **Résultat : E**xclusion devices du réseau

Quelles seraient les conséquences s’il réussirait ?: (conséquences par attaque)

Attaque	Impact Immédiat	Conséquence Métier	Coût Estimé
ADR **ADR Manipulation**	• Devices inefficaces • Collisions réseau • Portée réduite	• Données critiques perdues • Zones aveugles • Maintenance urgente	50K-200K€
SYNC **Beacon Synchronization**	• Désynchronisation générale • Communications chaotiques	• Usine paralysée • Ville désorganisée • Contrôle impossible	100K-500K€
FCNT **Frame Counter Attack**	• Contournement chiffrement • Injection données fausses	• Décisions erronées • Accidents industriels • Sécurité compromise	200K-1M€+

Quelles seraient les conséquences s’il réussirait ?: (conséquences par attaque)

MAC **MAC Command Injection**	• Contrôle devices à distance • Reconfiguration malveillante	• Sabotage industriel • Persistance attaquant • Escalade attaques	**75K-300K€**
SF **SF Targeting Attack**	• Dégradation ciblée • Devices sélectifs HS	• Services critiques hors ligne • Détection très difficile	**25K-100K€**
DC **Duty Cycle Exploitation**	• Bannissement réglementaire • Devices exclus réseau	• Amendes lourdes • Interruption service • Perte licence	**500K-2M€+**

Comment je vais me défendre ? (contre-mesures)

1- Manipulation d’ADR
- Validation cryptographique des commandes ADR
- Whitelist des paramètres ADR autorisés
- Monitoring des changements de Data Rate
- Alertes sur modifications suspectes

2- Synchronisation de Beacon
- Authentification forte des beacons
- Certificats numériques pour les gateways
- Monitoring temporel de la synchronisation
- Détection de dérive horaire anormale

3- Attaque de frame counter
- Politique stricte : rejet FCNT ≤ valeur stockée
- Surveillance des écarts de séquence
- Journalisation des reset FCNT
- Analyse des patterns de rejeu

4- Injection d’une commande Mac
- Chiffrement des commandes MAC
- Liste blanche des commandes autorisées
- Validation de la source des commandes
- Audit des modifications de configuration

5- Attaque SF targeting
- Frequency Hopping (FHSS)
- Détection de brouillage sélectif
- Adaptation automatique des SF
- Surveillance des interférences

6- Exploitation de duty cycle
- Rate limiting des commandes downlink
- Quotas d'utilisation du réseau
- Monitoring du temps d'émission
- Alertes risque réglementaire

Comment je vais me défendre ? (Architecture de défense)

Sécurité réseau

Authentification mutuelle devices/réseau
Chiffrement bout-en-bout des données
Rotation régulière des clés de session
Segmentation du réseau

Surveillance continue

Analyse comportementale des devices
Détection d'anomalies en temps réel
Corrélation des événements de sécurité
Journalisation forensique

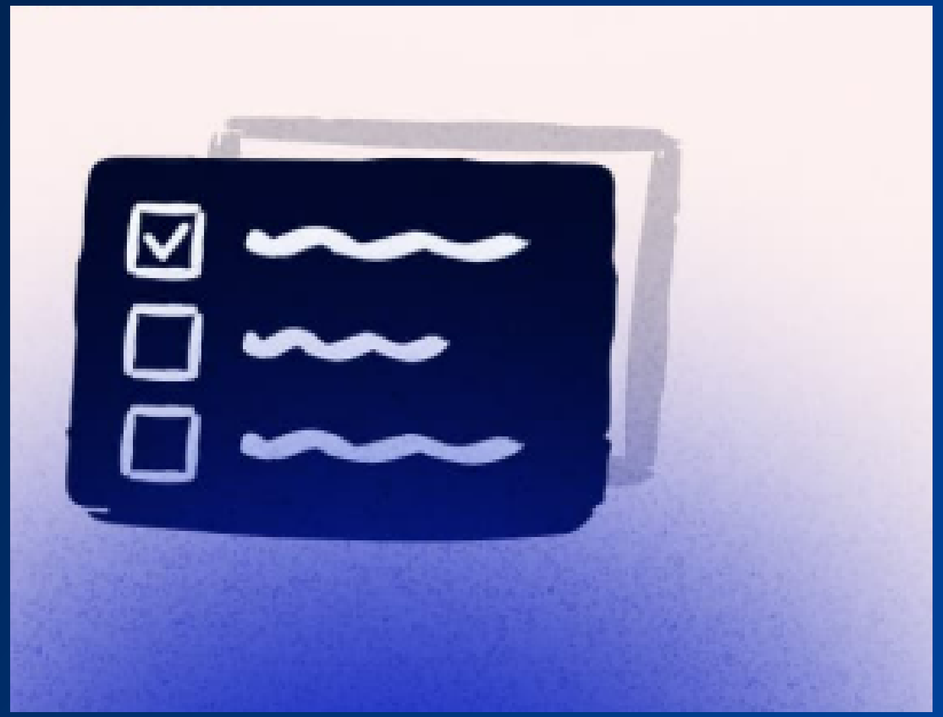
Réponse incident

Isolation automatique des devices compromis
Blocage des attaques en cours
Rétablissement rapide des services
Amélioration continue des défenses

CAHIER DES CHARGES FONCTIONNEL ET TECHNIQUE

Exigences fonctionnelles:

- Intégration d'attaques existantes
- Développement de nouvelles attaques LoRa
- Catalogue d'attaques avec descriptions
- Configuration paramétrable des attaques
- Lancement des attaques (dans le labo)
- Rapport des logs JSON

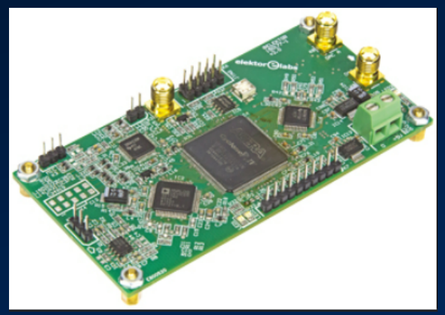


CAHIER DES CHARGES FONCTIONNEL ET TECHNIQUE

Cahier des charges techniques

Composants hardware:

- Radio: Cartes SDR (USRP, HackRF, LimeSDR)
- Gateways: Passerelles LoRa compatibles
- Devices: Capteurs IoT LoRa variés
- Réseau: Switch managé + isolation réseau

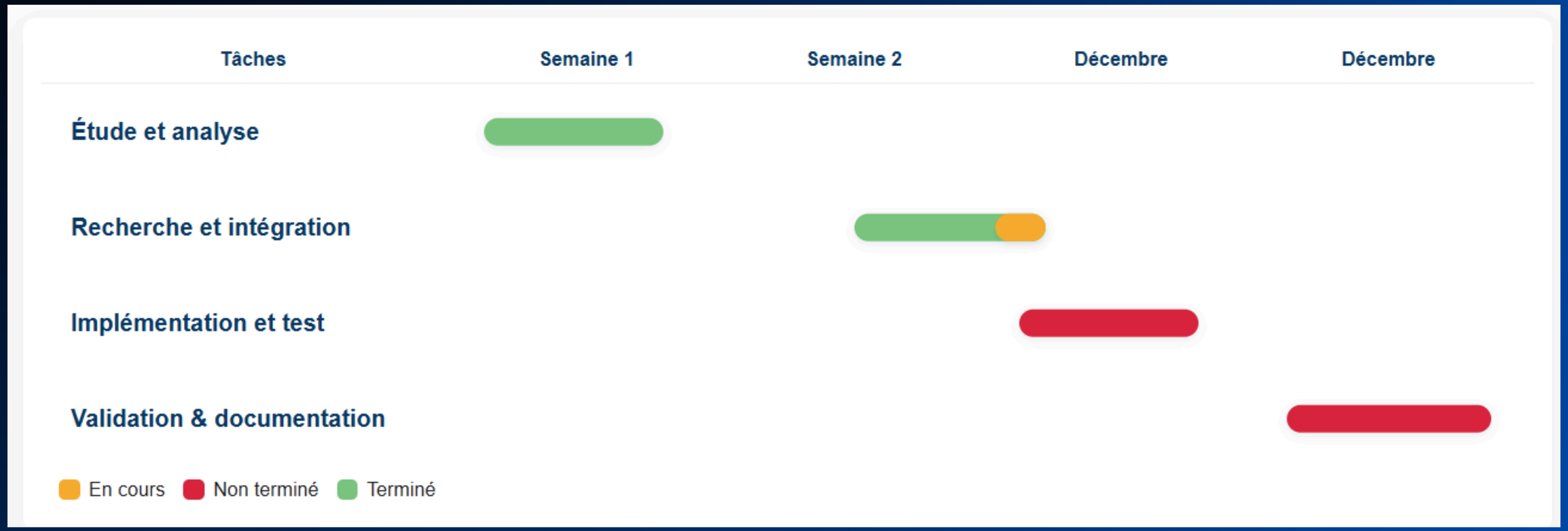


logiciel:

- OS: windows/ linux
- Langages: Python, C++ (arduino IDE), Bash
- Outils Radio: GNU Radio, gr-lora
- Network Server/Stack LoRaWAN : ChirpStack (open-source)
- Base de données & UI : PostgreSQL / InfluxDB + Grafana pour logs et visualisation

ChirpStack

RETRO PLANNING



AVANCEMENT

Etat de l’art

Analyse des Solutions Existantes

- Étude plateformes sécurité IoT (Kismet, Wireshark IoT)
- Analyse outils attaques LoRa (gr-lora, LoRaCrack)
- Revue académique attaques LoRaWAN récentes

Veille Technologique

- Protocoles LoRaWAN 1.0.3 & 1.1
- Faiblesses sécurité identifiées
- Contre-mesures documentées
- Réglementation spectre radio

SUITE À VENIR...