ANALYTICS TRACKER

Implémentation d'une Attaque par Canal Auxiliaire sur WhatsApp
(Side-Channel Timing Attack)

Documentation Technique & Scientifique

10 décembre 2025

Résumé

Ce document détaille l'architecture technique et les fondements scientifiques du projet *Analytics Tracker*. Il s'agit d'une preuve de concept (PoC) démontrant comment les accusés de réception techniques (Delivery Receipts) des applications de messagerie chiffrée peuvent être exploités pour inférer l'état d'activité d'un utilisateur (En ligne, En veille, Éteint, Déverrouillé) sans déclencher de notification.

Crédits et Origines

Ce projet est un fork évolué basé sur le travail original de **Gommzy Studio**.

— **PoC Original :** *Device Activity Tracker* par Gommzy Studio
— **Repo Source :** `https://github.com/gommzystudio/device-activity-tracker`
— **Recherche Fondamentale :** Basé sur le papier *"Careless Whisper"* (2024) par Gegenhuber et al.

Table des matières

1 Fondements Scientifiques

1.1 Le Vecteur d'Attaque : RTT

Le principe repose sur la mesure du temps aller-retour (*Round Trip Time*) d'un paquet de données envoyé aux serveurs de WhatsApp et relayé vers l'appareil cible. Le protocole oblige l'appareil à renvoyer un accusé de réception technique (ACK) pour confirmer la réception, même si l'utilisateur a masqué son statut en ligne.

1.2 La Signature Temporelle des États

L'attaque exploite les différences de latence induites par l'état énergétique du processeur du smartphone cible :

- **ONLINE (Actif) :** Le processeur est éveillé. Traitement immédiat ($< 1500ms$).
- **IDLE (Veille) :** Le téléphone est verrouillé. Le réveil du modem radio introduit une latence ($1500ms - 5000ms$).
- **OFFLINE :** Appareil éteint ou hors réseau. Aucun ACK renvoyé ($> 5000ms$).

1.3 La Technique du "Ghost Ping"

Pour rester furtif, le système envoie des **Réactions (Emojis)** liées à des identifiants de messages inexistants. L'application cible rejette la réaction silencieusement (pas de notification), mais le réseau a déjà renvoyé l'accusé de réception que nous mesurons.

2 Algorithmes de Traitement du Signal

2.1 Lissage Statistique (Médiane)

Les réseaux mobiles étant instables (jitter), nous n'utilisons jamais une valeur brute. Le système calcule en temps réel la **Médiane** sur une fenêtre glissante de 5 mesures. Cela permet d'ignorer les pics de lag isolés qui créeraient de faux positifs.

2.2 Détection Z-Score (Déverrouillage)

Le système utilise une analyse de déviation pour identifier l'événement **UNLOCKED** (passage de Veille à Actif). Il calcule dynamiquement la ligne de base (moyenne des 30 dernières mesures) et la volatilité habituelle de la connexion. Si la latence chute brutalement en dessous de la marge de variation normale, cela indique un réveil processeur provoqué par l'utilisateur.

2.3 Détection Circadienne (Sommeil)

Le système analyse l'historique des sessions pour identifier les "trous" d'activité supérieurs à 3600 secondes (1 heure), permettant de modéliser les cycles de sommeil de la cible.

3 Limites et Risques

Le système opère en **Mode Haute Précision** avec une fréquence de sondage fixe de 400ms. Bien que cela permette une résolution temporelle fine, ce motif de trafic robotique expose le numéro sondeur à un risque élevé de bannissement temporaire (Soft Ban) par les algorithmes de protection de WhatsApp.