ANALYTICS TRACKER

Implementation of a Side-Channel Timing Attack on WhatsApp

Technical & Scientific Documentation

December 10, 2025

Abstract

This document details the technical architecture and scientific foundations of the *Analytics Tracker* project. It is a Proof of Concept (PoC) demonstrating how technical delivery receipts in encrypted messaging applications can be exploited to infer a user's activity state (Online, Idle, Offline, Unlocked) without triggering any notification.

Credits and Origins

This project is an evolved fork based on the original work of **Gommzy Studio**.

- **Original PoC:** *Device Activity Tracker* by Gommzy Studio
- **Source Repo:** `https://github.com/gommzystudio/device-activity-tracker`
- **Fundamental Research:** Based on the paper *"Careless Whisper"* (2024) by Gegenhuber et al.

Contents

1 Scientific Foundations

1.1 The Attack Vector: RTT

The principle relies on measuring the Round Trip Time (RTT) of a data packet sent to WhatsApp servers and relayed to the target device. The protocol mandates the device to return a technical delivery receipt (ACK) to confirm reception, even if the user has hidden their "Online" or "Last Seen" status.

1.2 Temporal Signature of States

The attack exploits latency differences induced by the energy state of the target smartphone's processor:

- **ONLINE (Active):** The processor is awake. Immediate processing ($< 1500ms$).
- **IDLE (Standby):** The phone is locked. Waking up the radio modem introduces latency ($1500ms - 5000ms$).
- **OFFLINE:** Device turned off or out of network coverage. No ACK returned ($> 5000ms$).

1.3 The "Ghost Ping" Technique

To remain stealthy, the system sends **Reactions (Emojis)** linked to non-existent message IDs. The target application silently rejects the reaction (no notification), but the network layer has already returned the delivery receipt that we measure.

2 Signal Processing Algorithms

2.1 Statistical Smoothing (Median)

Mobile networks being unstable (jitter), we never use a raw value. The system calculates the **Median** in real-time over a sliding window of 5 measurements. This filters out isolated lag spikes that would create false positives.

2.2 Z-Score Detection (Unlocked Event)

The system uses deviation analysis to identify the **UNLOCKED** event (transition from Standby to Active). It dynamically calculates the baseline (median of the last 30 measurements) and the usual connection volatility. If the latency drops sharply below the normal variation margin, it indicates a processor wake-up triggered by the user.

2.3 Circadian Detection (Sleep)

The system analyzes session history to identify activity gaps exceeding 3600 seconds (1 hour), allowing for the modeling of the target's sleep cycles.

3 Limitations and Risks

The system operates in **High Precision Mode** with a fixed polling frequency of 400ms. While this allows for fine temporal resolution, this robotic traffic pattern exposes the probing number to a high risk of temporary banning (Soft Ban) by WhatsApp's protection algorithms.

4 Legal Disclaimer

This software is a Proof of Concept (PoC) for educational and research purposes only. Using this tool to monitor third parties without their explicit consent is illegal and punishable by law in most jurisdictions.