

# PAINE24 - Workshop

Physical Investigation of Smartphones:  
Is Side-Channel Analysis Still Effective?

Lionel Rivière - PhD



## Abstract

Smartphones are not only cutting-edge technology but also prime targets in security investigations. As they advance year by year, incorporating innovations such as smaller lithography sizes, package-on-package components, shielding, and anti-tampering measures, they present ever-increasing challenges for security experts.

It would be overly simplistic to claim that modern smartphones can be compromised solely through physical attacks. Investigating these devices demands a blend of expertise in both software and hardware reverse engineering.

In this workshop, we will demonstrate, using two different generations of smartphones, that despite technological advancements, Side Channel Analysis remains a powerful tool for compromising embedded cryptographic libraries when properly executed.

This interactive session will explore the techniques and methodology required to conduct Side Channel Analysis on cryptographic implementations, using a Nexus 5 and a Pixel 8 as case studies. Live EM acquisition will be performed on prepared devices, though no hands-on exercises are planned for participants.