



Leaking Power Signals Remotely on Android

Advisor: **Mathias Oberhuber**

Motivation

Mobile phones running Android expose various sensor signals to unprivileged apps and to the browser. These signals include power-related information that attackers can exploit to mount power side-channel attacks and leak sensitive data. This work aims to mount such attacks remotely by abusing signals transmitted to a third party (e.g., audio during a phone call) to extract sensitive information from a user.

In this thesis, you will extend an existing proof-of-concept implementation to a remote attack.

Goals and Tasks

-  Learn about prior work on power and power-related side channels on Android.
-  Build/extend a prototype to collect audio-based power signals on Android.
-  Evaluate if these signals can be exploited remotely (e.g., over a phone call).
-  Perform an attack



Literature

- > [M. Oberhuber et al.](#)
Power-Related Side-Channel Attacks using the Android Sensor Framework
[NDSS](#)
- > [D. Genkin et al.](#)
Lend me your ear: Passive remote physical side channels on PCs
[31st USENIX Security Symposium \(USENIX Security 22\)](#)

Courses & Deliverables

- ☒ **Introduction to Scientific Working**
Short report on background
Short presentation
- ☒ **Bachelor Project**
Project code and documentation
- ☒ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

- ☒ CS ☒ ICE ☒ SEM

Prerequisites

- > Interest in mobile security
- > Basic knowledge of mobile App development (Android, C++, Python)

Advisor Contact

mathias.oberhuber@tugraz.at