Electromagnetic Interference Experiments: Design and Best Practices

Marcell Szakály, Sebastian Köhler, Martin Strohmeier, Ivan Martinovic

LASER @ ACSAC 2024

2024-12-10



UNIVERSITY OF OXFORD

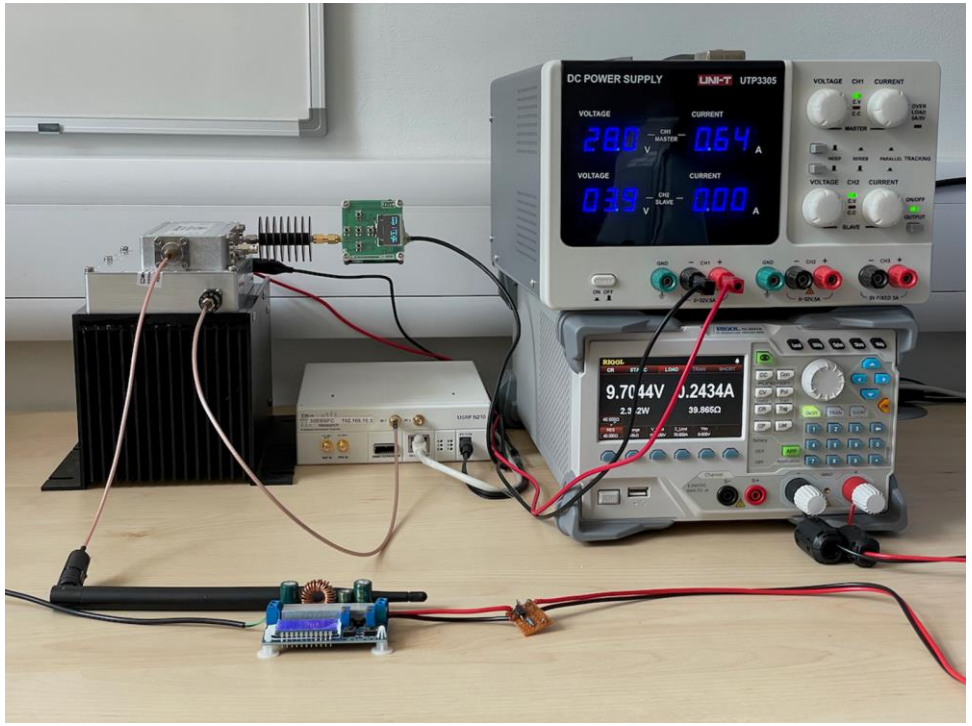
SSL

Systems Security Lab

Introduction

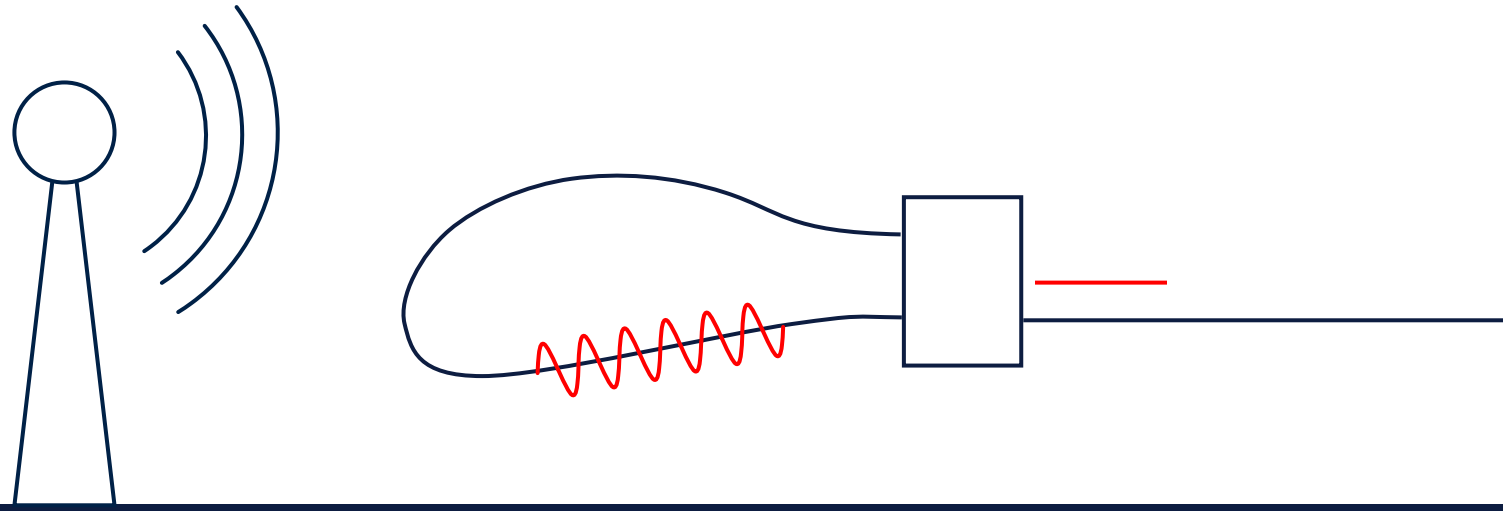
- EMI is an active research area
- Hardware focused, physical experiments
- Potential issues with experimental design
- Reproducibility difficult
- Necessary to be transparent about experiments

- In this talk
  - Introduce EMI
  - Explain experimental pitfalls
  - Discuss issues after publication: negative results, reproducibility



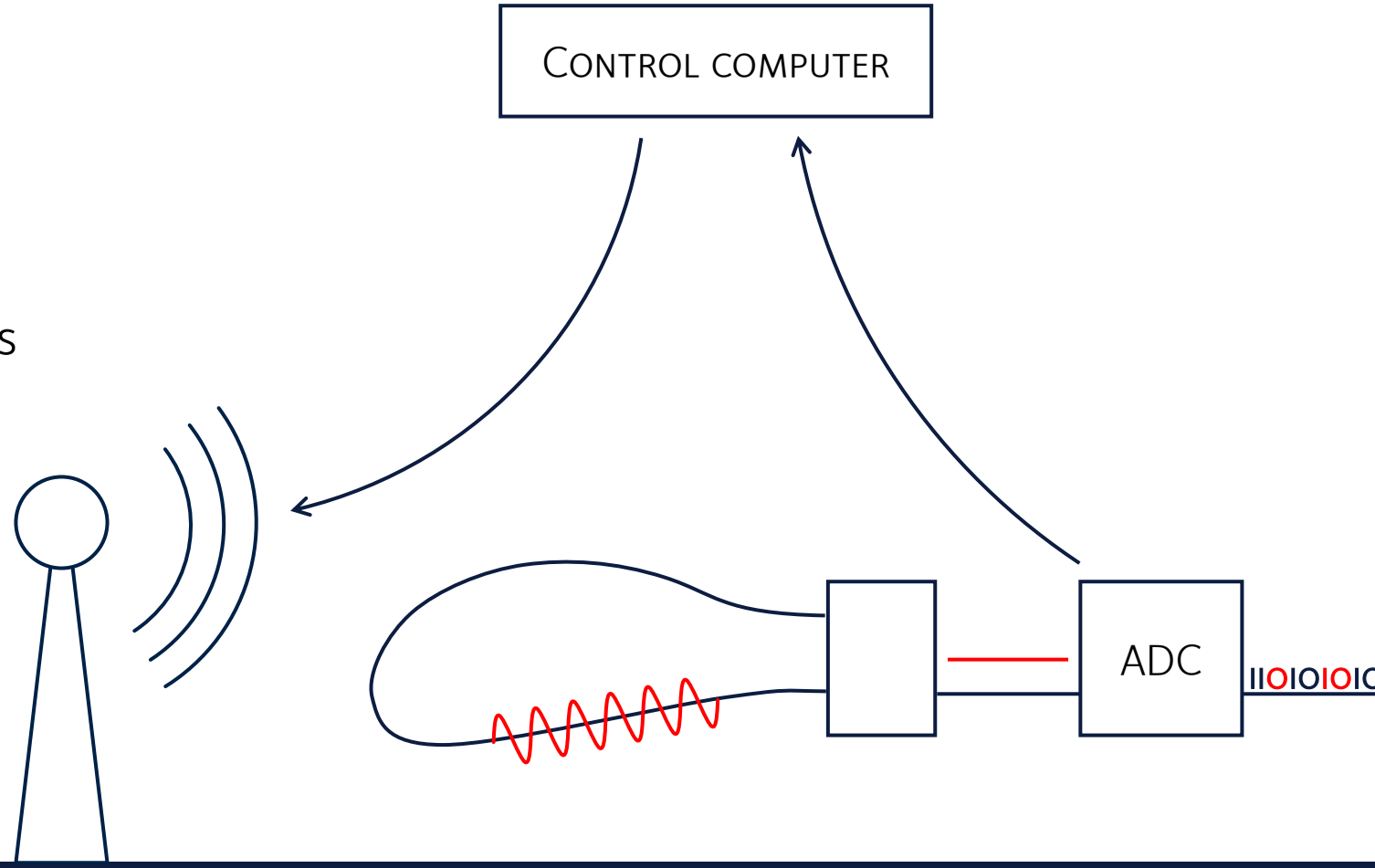
EMI Attacks

- All wires are antennas
- Wires in devices are unintended antennas
- External RF signal induces voltage in wires
- Common circuits act as unintended demodulator
- DC offset on wires inside device
- Internal wires carry important analog signals



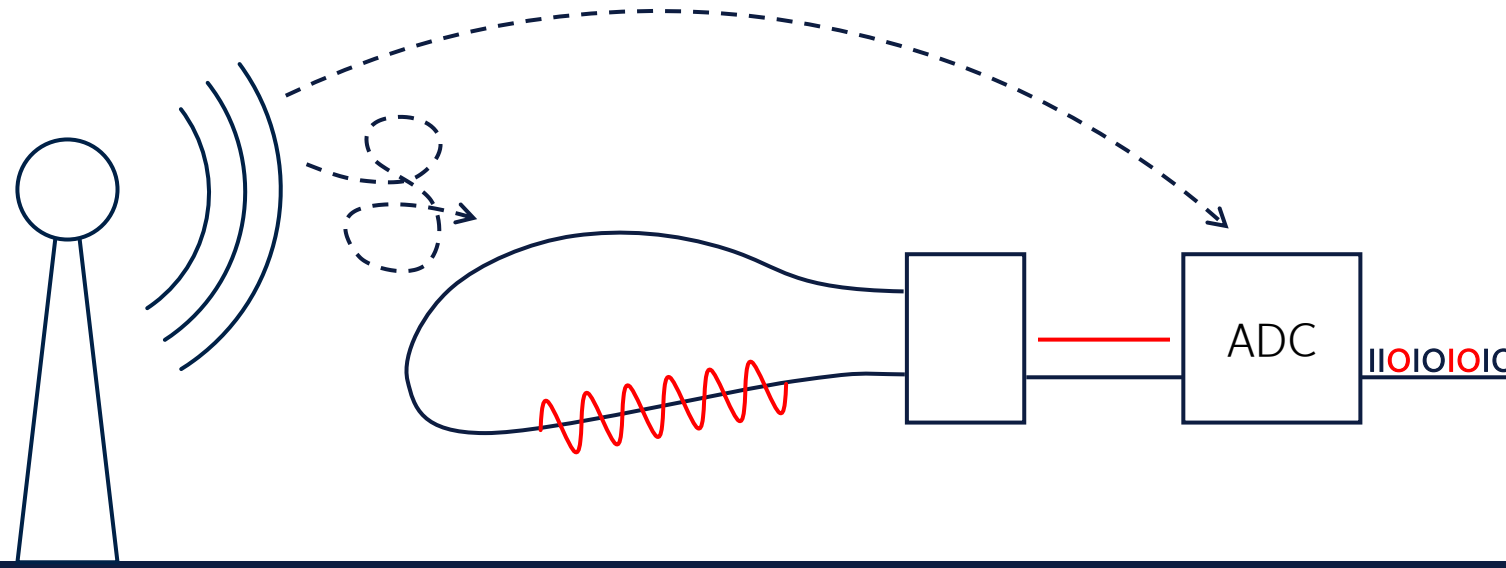
EMI Measurements

- Analog systems
  - e.g., amplifiers
  - Connect to external “lab” ADC
- Digital systems:
  - e.g., camera
  - ADC already integrated in device
- Control RF source, record measurements



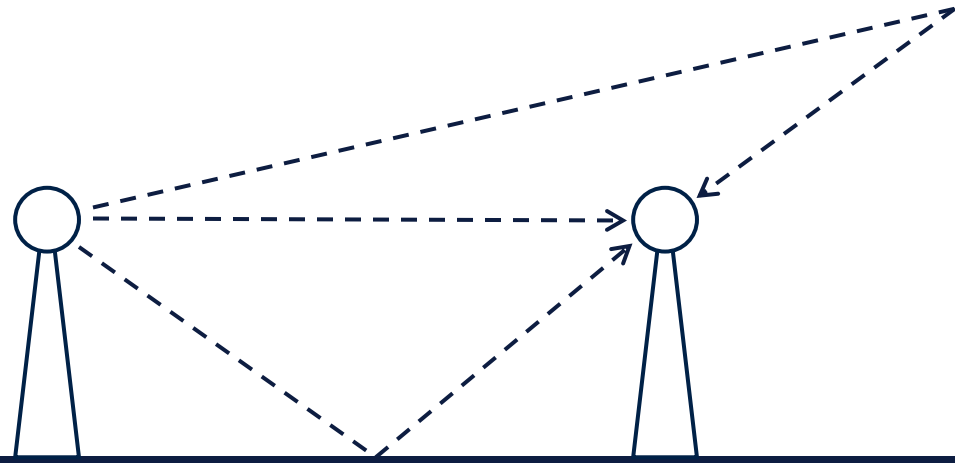
EMI Measurement Issues

- Multipath propagation
- Unintended coupling
  - Wired coupling instead of wireless
  - Impacts range results
- Unintended target
  - Wired or Wireless
  - Affects lab equipment instead of DUT



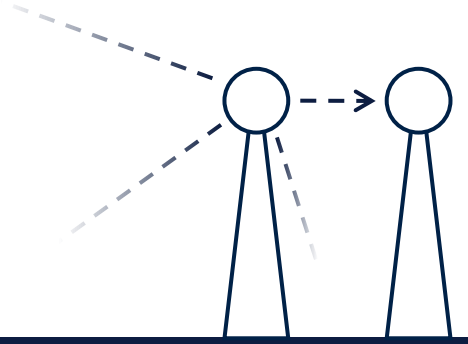
Multipath Interference

- Exact results may be very sensitive to geometry → hard to reproduce
- To eliminate, must minimize reflections
  - Reduce power
  - Reduce distance
  - Use anechoic chamber



Multipath Interference

- Exact results may be very sensitive to geometry → hard to reproduce
- To eliminate, must minimize reflections
  - Reduce power
  - Reduce distance
  - Use anechoic chamber
- But, we want realistic attacks
  - At high power
  - Long range
  - In real environment
- Determine what is best for each experiment
  - Need to change setup very carefully to make numeric comparisons



Unintended Coupling

- Signal can couple into shared wires, and travel with lower loss than wireless
  - Data wires
  - Powerlines
- Minimize cables between source and target side
  - Air gap if practical
- Minimize cables inside the RF beam
  - Also think about area behind device

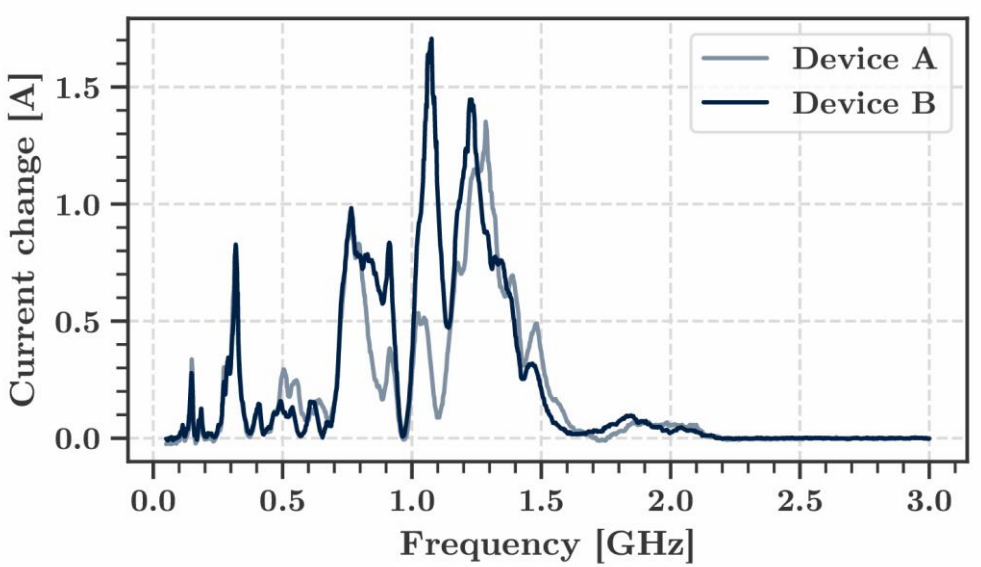


Unintended Target

- Insulate lab equipment
  - Ferrite chokes
  - Separate power supply
  - Place away from RF beam
- Use immune equipment
  - Best choices: Oscilloscopes, professional lab equipment
  - Worst choices: Arduino ADC, multimeter
- Redundant measurements
  - Very unlikely to be effected the same

Reproducibility

- Each device has very different response
  - Must compare to identical device
- Signal source should be very similar
  - Report entire RF chain
  - Source, Amplifier, Antenna
  - Measure TX power level
- Multipath aspect very hard to replicate
  - Only well controlled environments



- Identical devices in same environment will behave largely the same
- We show in Appendix our frequency response plots
- We publish the raw data used to plot
  - https://github.com/ssloxford/assault_and_battery

Negative Results

- Some targets have no measurable response
- Very easy to buy many devices and cherrypick
- Important to share results about all devices
- How can we encourage all results to be published?
- What if entire device class is immune?

Data Collection Software

- Developed Python library
- Connects to SDRs, frequency generator
- Connects to Oscilloscope, DC load
- Run parametric sweeps, collect data
- Supports Wi-Fi airgap between RF source and measurement hardware
- Available as one of our artifacts
  - https://github.com/ssloxford/emi_experiment_lib



Points for Discussion

- How can we increase reproducibility?
  - Results specific to hardware
  - Potential environmental factors
- How to encourage publishing negative results?
  - Both single experiments and entire papers

Thank you for your attention!

https://github.com/ssloxford/assault_and_battery

marcell.szakaly@cs.ox.ac.uk



UNIVERSITY OF OXFORD

SSL Systems Security Lab