Threat potential assessment of power management related data leaks

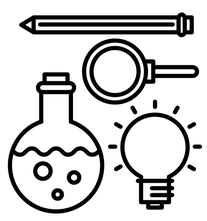
Philipp Miedl

miedlp@ethz.ch

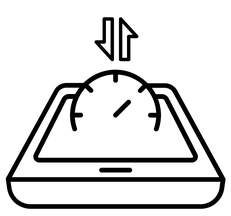
Computer Engineering and Networks Laboratory

ETH zürich

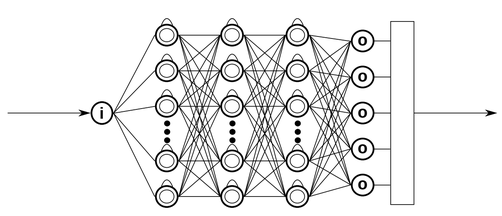
Contributions



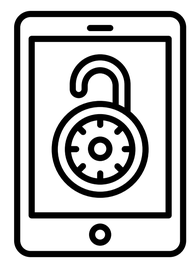
Analysis methodology for data leak threat potential assessment



Capacity bound derivation methods for continuous and discrete covert channels



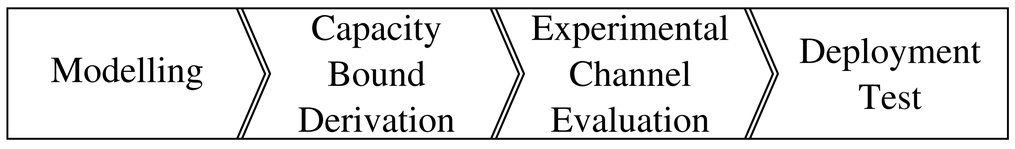
Recurrent neural network based signal decoder for discrete covert channels



Thermal side channel attack for extraction of runtime information

Data Leak Threat Potential Assessment

- Analysis methodology to evaluate covert channels [1]
- Allows to assess the threat potential of data leaks



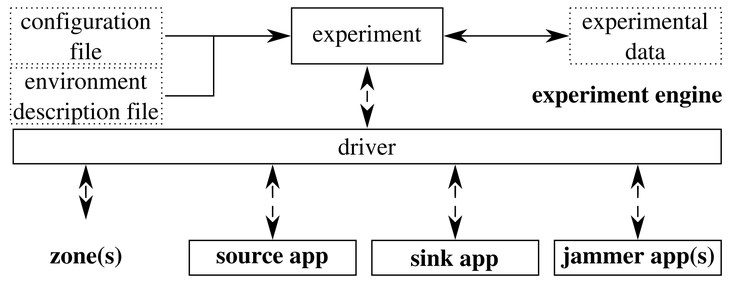
- Supports reproducibility, comparability and expressiveness of results
- The Experiment Orchestration Toolkit (ExOT) implements this analysis methodology

Experiment Orchestration Toolkit (ExOT)

Software toolkit to support researchers in experiment generation, execution & analysis

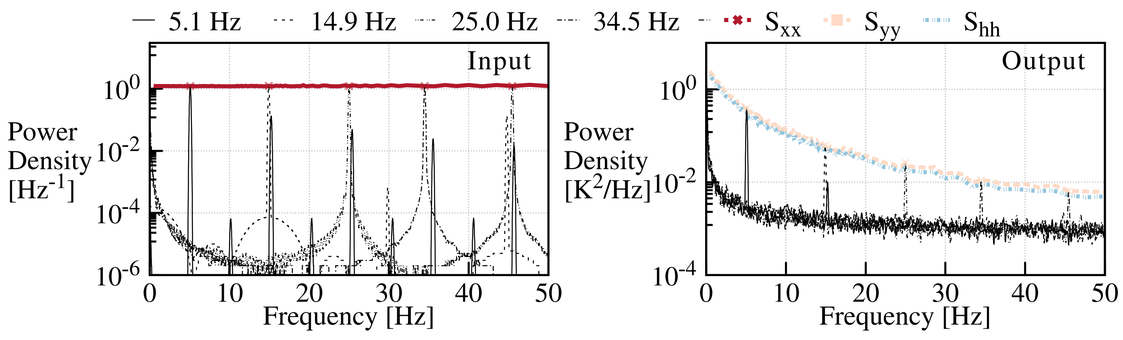
Powered by: C++ Java python [T]

Available online



Capacity of Continuous Covert Channels

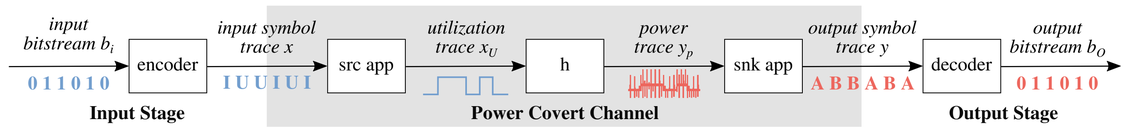
- Define set of experiments based on hardware characteristics & the channel model, e.g. thermal covert channel [2]
- Determine power spectra based on the experiments



- Derive channel capacity bound with water-filling algorithm

Capacity of Discrete Covert Channels

- Establish channel model, e.g. power covert channel [3]



- Determine state transition matrix **A** and state transition time t
- Calculate upper channel capacity bound:

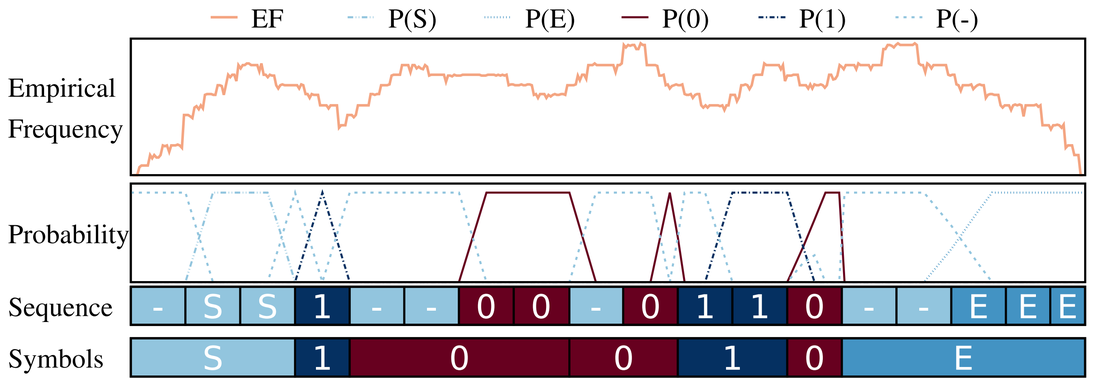
$$C = \log_2 \lambda_1 \text{[bits per channel use]} \quad B_{\max} = \frac{C}{T_s} \text{[bits per second]}$$

λ_1 ... prinicpal right eigenvalue of the transition matrix **A**

T_s ... symbol duration (best case)

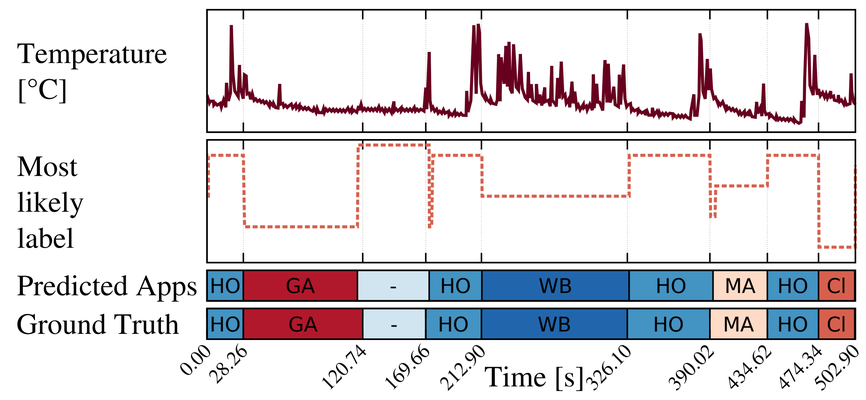
Symbol Decoding using RNN

- Long Short-Term Memory (LSTM) based symbol decoder for frequency covert channel [4]
- Applies connectionist temporal classification (CTC)
- Compensates timing and value variations of symbols



Thermal Side Channel

- Unrestricted access to temperature of mobile devices poses security & privacy risk [5]
- Temperature analysis using sequence-to-sequence labelling techniques allows detection of other applications on device



[1] P. Miedl, B. Klopott, and L. Thiele, “Increased reproducibility and comparability of data leak evaluations using ExOT,” in 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2020.
[2] D. B. Bartolini, P. Miedl, and L. Thiele, “On the Capacity of Thermal Covert Channels in Multicores,” in Proceedings of the Eleventh European Conference on Computer Systems, ser. EuroSys ’16. New York, NY, USA: ACM, 2016, pp. 24:1–24:16.
[3] P. Miedl and L. Thiele, “The Security Risks of Power Measurements in Multicores,” in Proceedings of the 2018 ACM symposium on Applied computing. ACM, 2018.
[4] P. Miedl et al., “Frequency Scaling as a Security Threat on MulticoreSystems,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 11, pp. 2497–2508, 2018.
[5] Manuscript in preparation.