

ETH zürich





**Increased reproducibility and comparability of data leak evaluations using ExOT**

P. Miedl, B. Klopott and L. Thiele  
DATE 2020


ETH zürich

P. Miedl, B. Klopott and L. Thiele DATE 2020 11.03.2020 1

Why is data leak evaluation important?

<https://networkencyclopedia.com/virtualization/> Screenshot [www.android.com](http://www.android.com)



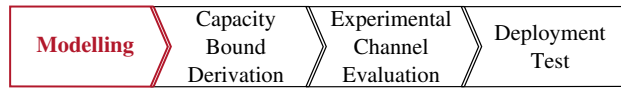
2

Which weaknesses do recently published evaluations have?

- ✗ Required engineering & time effort leads to **non-exhaustive** analyses to save resources
- ✗ **Not-expressive** results lead to misclassification of threat potential of data leak, e. g. thermal covert channel
- ✗ Different metrics lead to **not-comparable** results and need for expensive re-evaluation, e. g. cache covert channels

3

Methodology for exhaustive data leak evaluation



4

Derive a formal channel model

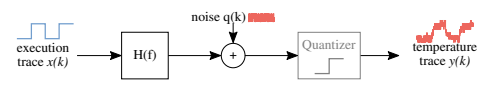
Beneficial for defining evaluation **metrics**, e. g. channel capacity bound

Requires experiments for channel exploration

Relies on **researcher expertise**

5


Example: Thermal Covert Channel



Modelled as **continuous** covert channel

6

Methodology for exhaustive data leak evaluation



7

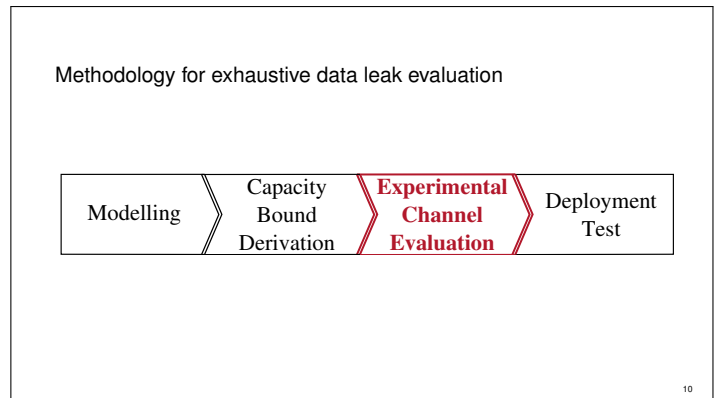
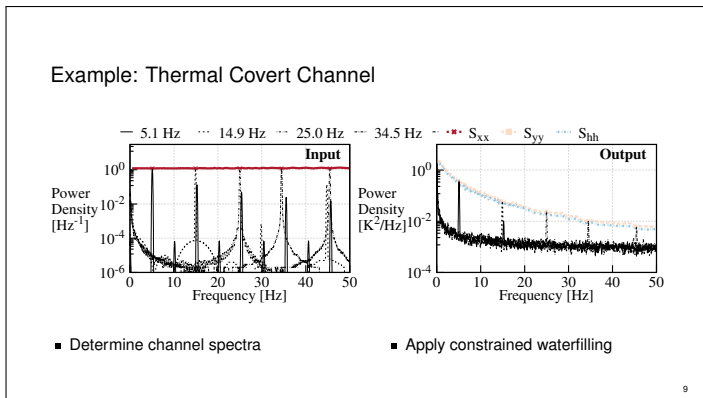
Derive capacity bound as comparable metric

Capacity bound **independent from implementation** artifacts

Allows to **assess** the **threat potential** of a covert channel

Method to derive bound **depends on channel model**

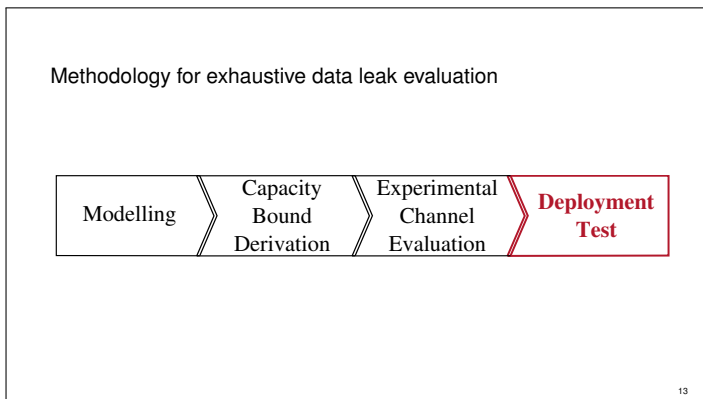
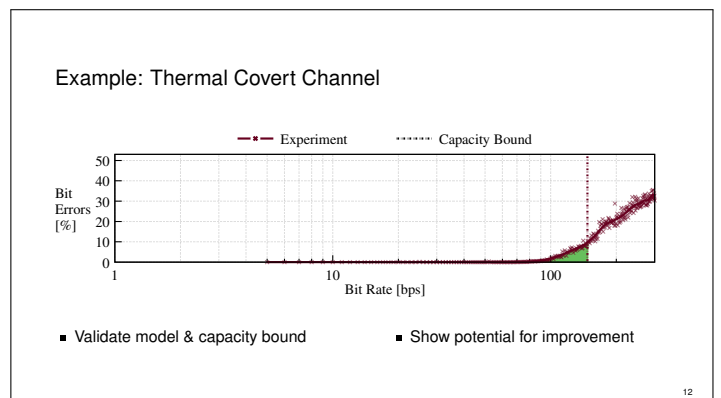
8



### Validate model and capacity bound with experimental evidence

Experiments conducted under **well defined laboratory conditions** for reproducibility

**Rudimentary communication channel** with or without interference



### Show a real world application

Real application based on previously gained knowledge

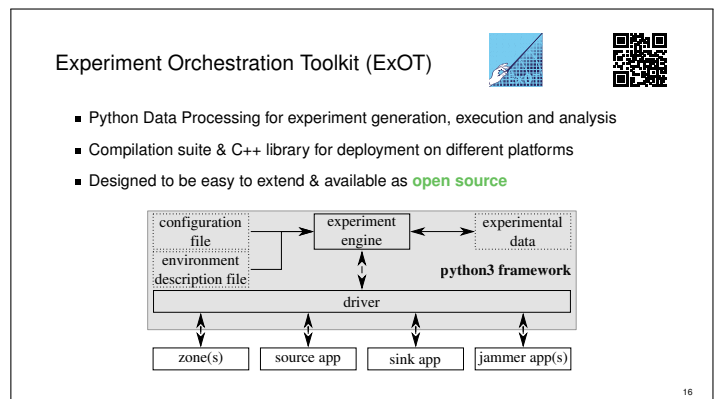
Environment not controlled and **highly application specific**

SSH communication channel over cache covert channel in the cloud by C.Maurice et al.<sup>1</sup>

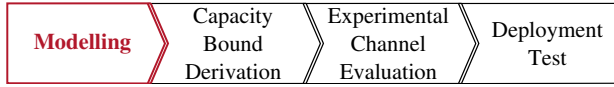
<sup>1</sup>C. Maurice et al., "Hello from the other side: SSH over robust cache covert channels in the cloud," NDSS, San Diego, CA, US, 2017.

### Which weaknesses do recently published evaluations have?

- ✗ Required engineering & time effort leads to **non-exhaustive** analyses to save resources
- ✗ **Not-expressive** results lead to misclassification of threat potential of data leak, e. g. thermal covert channel
- ✗ Different metrics lead to **not-comparable** results and need for expensive re-evaluation, e. g. cache covert channels



ExOT helps to implement the methodology by...



- ExOT provides **blueprints** for channels modelled as
- Time-continuous and value-continuous
- Time-discrete and value-discrete

17

ExOT helps to implement the methodology by...



- Provides **experiment flow**: experiment generation, execution and analysis
- Basic building blocks for measurement applications

18

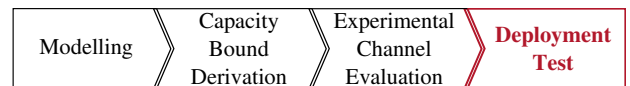
ExOT helps to implement the methodology by...



- Prescribed software flow** for experiments and environment handling
- Gathers vital experiment parameters
- Different options for rudimentary communication channel

19

ExOT helps to implement the methodology by...



- Basic **building blocks for deployment applications** can be reused

20

Using our methodology and ExOT in practice

Re-evaluation of known covert channels:

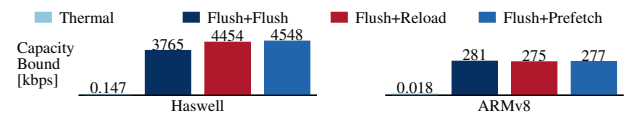
- Thermal
- Flush+Flush
- Flush+Reload
- Flush+Prefetch

Two distinct platforms:

- Lenovo T440p laptop; Intel i7-4700MQ (**Haswell**)
- NVIDIA Jetson TX2; quad-core ARM A57 cluster (**ARMv8**)

21

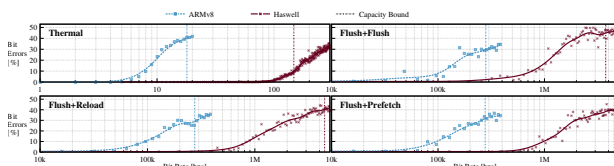
Capacity bounds derivation for different covert channels



**Fast assessment of threat potential & comparability of different covert channels**

22

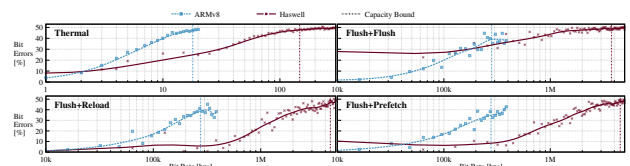
Performance without interference



**Low cost for scaling of experimental evaluation using ExOT**

23

Performance with interference



**Changing experiment parameters easy using ExOT**

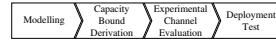
24

## Advantages of the proposed methodology implemented by ExOT

- ✓ ExOT **reduces** the required engineering & time **effort** for exhaustive data leak analyses
- ✓ The presented methodology implemented with ExOT supports **reproducibility**, **comparability** and **expressiveness** of analysis results
- ✓ Our methodology helps to derive fitting **models**, **metrics** and **experiments** for a data leak evaluation

25

## Methodology for data leak analysis



- ✓ Generally applicable to different classes of covert channels
- ✓ Helps defining models, metrics & experiments
- ✓ Reproducible, comparable & expressive results

## Experiment Orchestration Toolkit (ExOT)



- ✓ Python Data Processing for experiment generation, execution and analysis
- ✓ Compilation suite & C++ library for deployment on different platforms
- ✓ Open source and designed to be easy to extend

26