TTControl
HYDAC INTERNATIONAL

AI-accelerated Implementation Testing: Research vs Practice

OPTIMIST Hour

Jakub Breier
Senior Cyber Security Manager
TTControl GmbH, Vienna, Austria

jakub.breier@gmail.com
https://jbreier.com

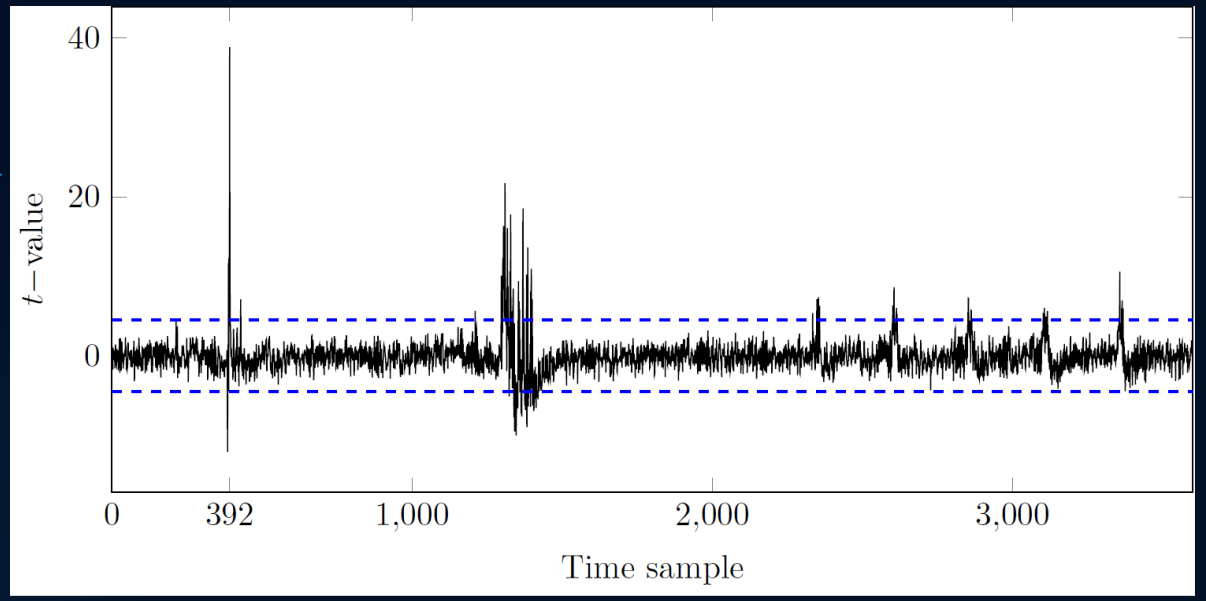
TTControl
HYDAC INTERNATIONAL

AI-accelerated Leakage Assessment

TTControl
HYDAC INTERNATIONAL

Leakage Assessment in Side-Channel Analysis

- Idea:
  - Determine whether an attacker can extract information from side-channel measurements
- Most popular methods:
  - Welch's *t*-test [1]
    → TVLA: Test Vector Leakage Assessment
  - Pearson's X^2-test [2]
- Modus operandi:
  - Collect two groups of side-channel measurements
    → fixed-vs-fixed or random-vs-fixed inputs
  - Check if the groups can be distinguished
    → If yes, informative side-channel leakage is present



Source: Hou, X. and Breier, J., 2024. Cryptography and Embedded Systems Security. Springer.

[1] Gilbert Goodwill, B.J., Jaffe, J. and Rohatgi, P., 2011, September. A testing methodology for side-channel resistance validation. In NIST Non-Invasive Attack Testing Workshop.
[2] Moradi, A., Richter, B., Schneider, T. and Standaert, F.X., 2018. Leakage detection with the X2-test. IACR Transactions on Cryptographic Hardware and Embedded Systems.

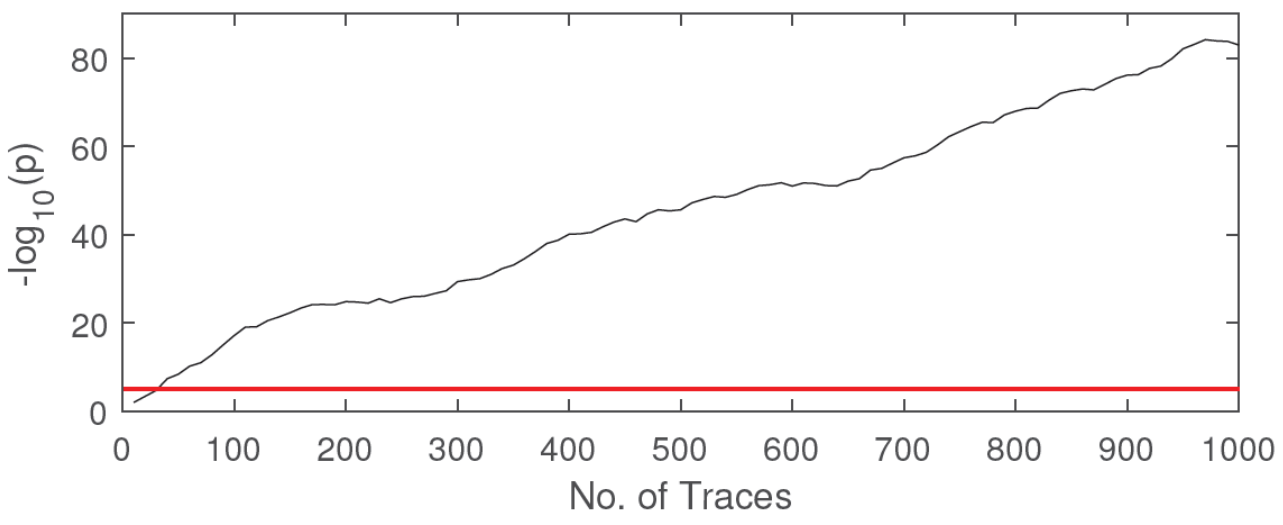
DL-LA: Deep Learning Leakage Assessment [1]

- Supervised approach
- Uses deep learning as a distinguisher between the two groups (fixed-vs-fixed or random-vs-fixed)
- Success rate of the classification on the validation set quantifies the amount of generalizable information that the model could extract from the training set during the training phase
  - Leakage is detected by using the training set
    → If we use 1000 traces for training and 5000 traces for validation and a leakage is found, we conclude that the implementation leaks with 1000 traces

- If the validation succeeds with a *better-than-random* guessing, we can conclude that informative side-channel information is present

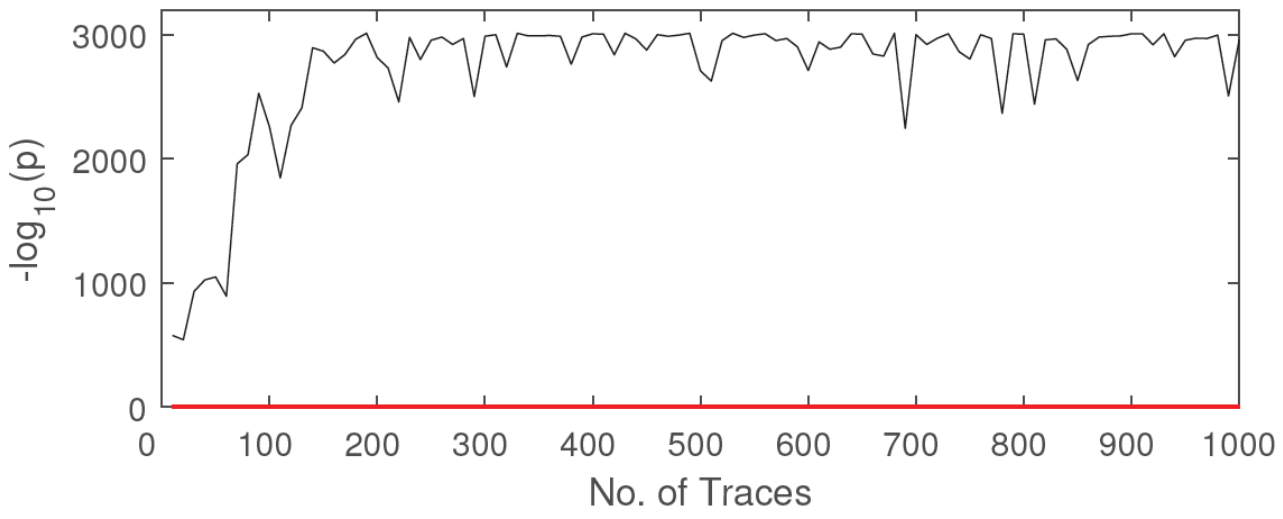
[1] Moos, T., Wegener, F. and Moradi, A., 2021. DL-LA: Deep Learning Leakage Assessment: A modern roadmap for SCA evaluations. IACR Transactions on Cryptographic Hardware and Embedded Systems, pp.552-598.

Unprotected PRESENT-80 Example



t-test

- Threshold 4.5 is crossed at 20 traces



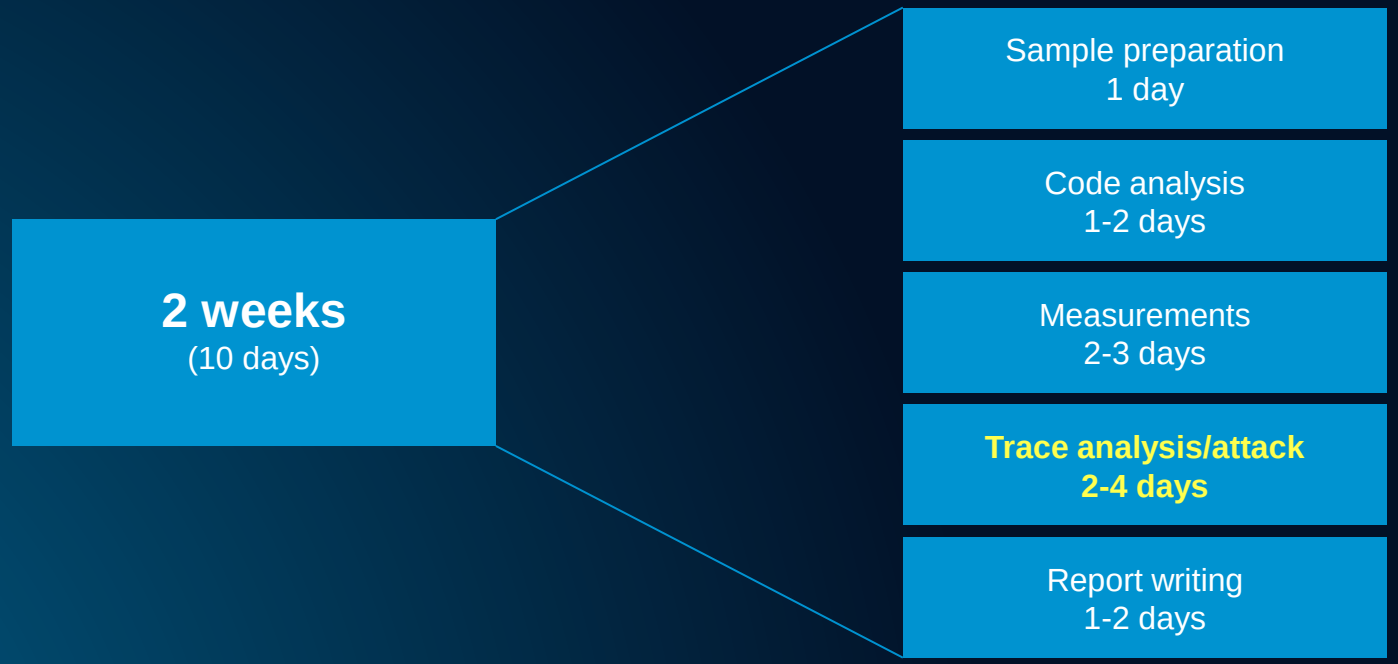
DL-LA

- 30 epochs per *p* value
- 10 000 validation traces
- Threshold is 4.5 is crossed at 10 traces (minimum)

Source: Moos, T., Wegener, F. and Moradi, A. DL-LA: Deep Learning Leakage Assessment: A modern roadmap for SCA evaluations. IACR TCHES 2021.

Payment Card Assessment

Standard Assessment Timeline



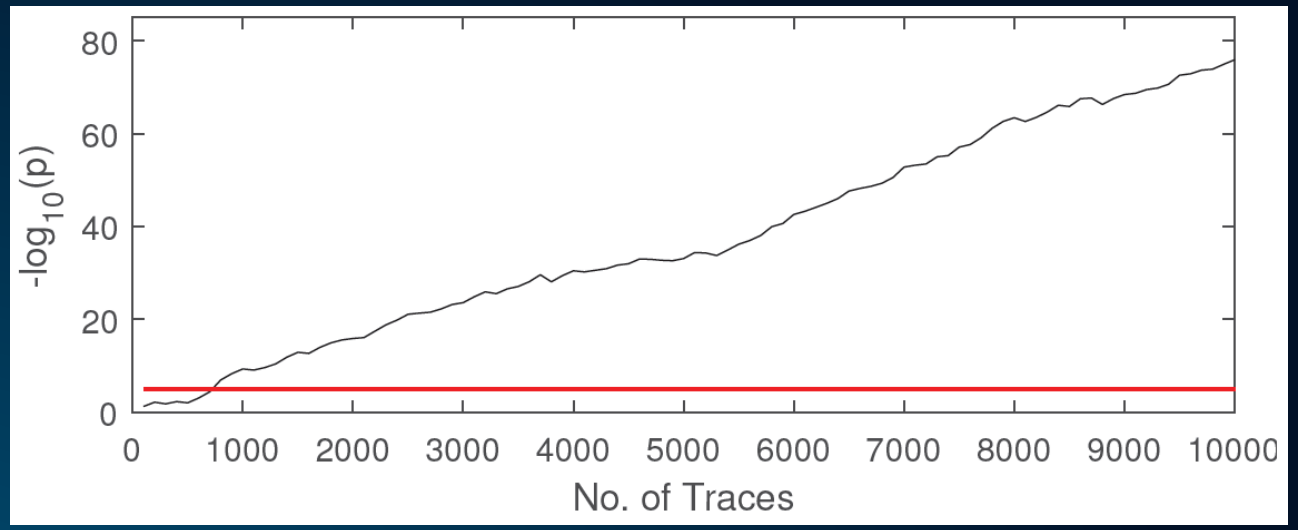
TTControl
HYDAC INTERNATIONAL

Standard Number of Traces

- Number of smart card samples: 5
- Transaction limit: 2^{15} (32,768) or 2^{16} (65,536)
- Maximum number of traces for all the samples: **163,840** or **327,680**
  - In reality, 1-2 samples might be destroyed during the decapsulation process
  - Many traces are wasted to find:
    → correct time location of the crypto algorithm execution
    → best spatial location for EM probe
  - As the samples have different secret keys, the traces anyway cannot be combined

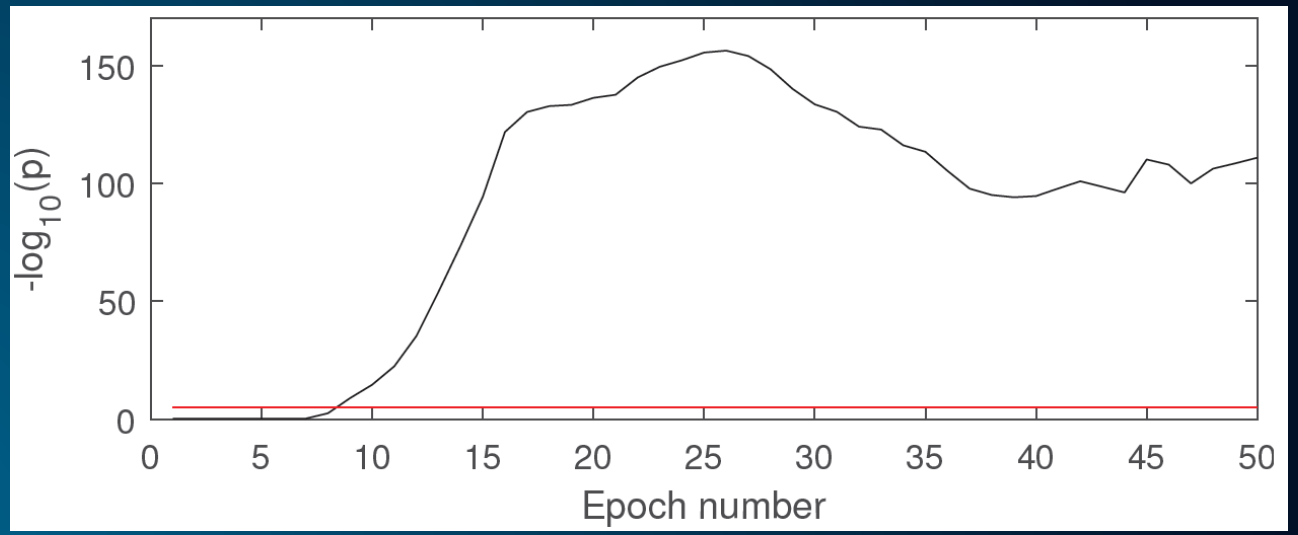
Adding Countermeasures

PRESENT-80 Software Threshold Implementation



2nd order *t*-test

- Threshold 4.5 is crossed at ~800 traces

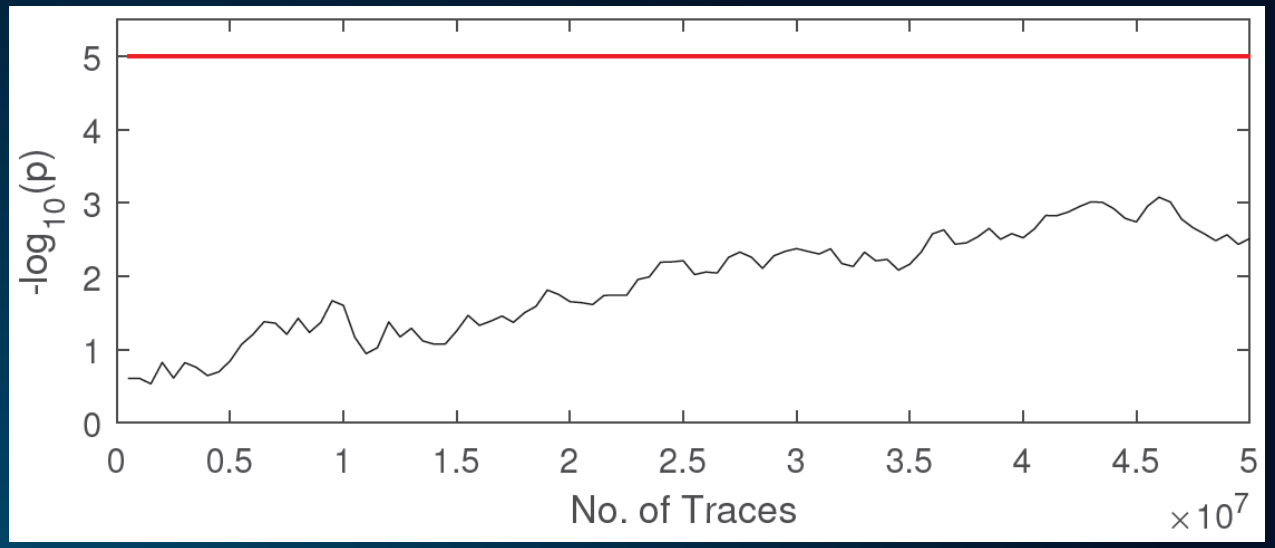


DL-LA

- 500 training traces
- 80 000 validation traces

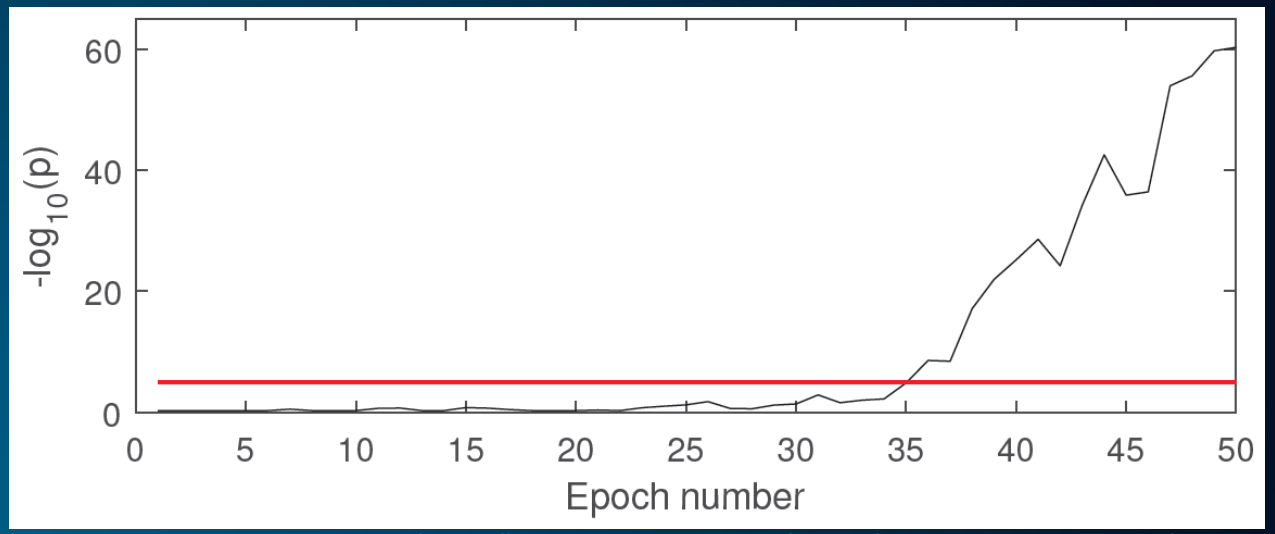
Source: Moos, T., Wegener, F. and Moradi, A. DL-LA: Deep Learning Leakage Assessment: A modern roadmap for SCA evaluations. IACR TCHES 2021.

PRESENT-80 Hardware Threshold Implementation



3rd order *t*-test

- No leakage detected with 50M traces



DL-LA

- 25M training traces
- 5M validation traces

Source: Moos, T., Wegener, F. and Moradi, A. DL-LA: Deep Learning Leakage Assessment: A modern roadmap for SCA evaluations. IACR TCHES 2021.

Discussion Points

Discussion Points

- Generally, DL-LA requires more traces for analysis compared to “traditional” methods
  - Validation set makes the difference
    - → Validation accuracy is dependent on the set size
    - → Would it be possible to reduce the set size by adjusting the approach?

- In hardware-protected case, t-test was not able to detect any leakage with 50M traces
- DL-LA detected leakage with 30M traces
  - Could a more efficient DL-based leakage assessment method be developed?

- Explainability
  - Would it be possible to find out the nature of the leakage by analyzing the trained model?

- At the moment, only one proposal has been developed (DL-LA), in 2021
  - More research in this direction would be welcome by the community

TTControl
HYDAC INTERNATIONAL

Thank you.

Follow us on

LinkedIn

ttcontrol.com